

HiPER 命令行配置手册

第 6 卷：业务管理

上海艾泰科技有限公司

http://www.utt.com.cn

版 权 声 明

产品编号（PN）：0900-0050-001

文档编号（DN）：PR-PMMU-1106.07-PPR-CN-1.0A

目 录

导　　读

命令行格式约定

本手册中，讲解命令句法时，英文字体为“ Times New Roman ”字体，中文字体为“ 宋体 ”。相关命令行格式约定的描述如下：

加粗字体：指配置命令时需要原封不动输入的参数。

倾斜字体：指配置命令时必须为之提供实际值的参数。

[ ]：表示用[ ]扩起来的部分，在配置命令时是可选的。

{x | y | … }：表示从两个或多个选项中选取一个。

[x | y | …]：表示从两个或多个选项中选取一个或者不选。

!：由感叹号！开始的行表示注释行。

_：输入光标位置。

>:命令行参数层次分隔符。

此外，在实际的配置实例和终端输出（Terminal Display）中，使用加粗“ Courier New ”字体表示用户从终端输入的信息；使用普通“ Courier New ”字体表示屏幕输出信息。

键盘操作约定

<>：表示键盘上的按键。例如，<Enter>表示回车。

<键 1+键 2>：表示在键盘上同时按下键 1 和键 2。例如，<Ctrl+H>表示同时按下 Ctrl 键和 H 键。

特殊符号约定

该符号表示提示信息，指出重点注意事项。

适用版本

本手册适用的软件版本为 ReOS 5.x。

第1章 业务管理功能介绍

1.1 概述

Internet 发展的同时也带来了一些副作用，如出现了赌博、色情等和国家法律法规相悖的网站；宽带网络给大众提供快速冲浪的同时，网络蠕虫病毒也得到快速传播，给电脑使用者带来很大的威胁。各个机构需要连接到 Internet，因此也制定了具体的上网规则，如某些地方规定公务员不能在上班时间炒股和通过即时消息聊天，企业不允许电脑使用者操作和工作无关的事情，家长需要能在指定的控制孩子的上网时间，蠕虫病毒和黑客攻击充斥网络，需要将它们挡在攻击电脑之前等，不一而足。

我们可以把整个网络分成三个层次，一个是核心层，接下来是汇聚层，和用户最接近的是接入层。因为管理的多样性，在接入层实施控制是理想的选择。一方面，可以根据各个机构的具体特点发展本机构特色的业务，另外一个方面，将大量的控制分散到接入层，对于汇聚和核心两个层次也是起到了分解压力的作用。

HiPER 系列的业务管理功能正是为解决这些问题而开发。

灵活地运用 HiPER 的业务管理功能，不仅能够为不同的用户设置不同的 Internet 访问权限，还可以控制用户在不同时段的 Internet 访问权限。在实际应用中，可根据各个机构的管理规则，然后制定出相应的业务管理策略，在 HiPER 上实施。如在学校使用 HiPER 作为宽带接入设备时，可设置学生不能访问游戏网站；而对于家庭来说，只在指定的时间内允许孩子上网；企业的财务部门的机器不能被互联网访问，对于各种攻击包括病毒的过滤等。

HiPER 的业务管理功能是根据用户定义的策略，监测流经 HiPER 的每个包，结合 HiPER 的防火墙技术 Filter 来实现的。Filter 的机制就是分析流经 HiPER 的数据包，针对数据包的特点，如源地址、目标地址、上层协议或其他信息，通过定义一些策略对经过路由器（网关）接口上的数据包进行控制：转发或丢弃。

对于 HiPER 而言，包有进入和外出两个方向。HiPER 系列产品所能处理的包可以是进入 HiPER，或者从 HiPER 往外出，对这些包的动作可以是转发，或者是丢弃。包的类型可以是基本的 IP 包，这个是基本的包过滤防火墙的功能，也可以是扩展的功能，如 Ethernet 包，还可以根据时间段来实施包的过滤动作。HiPER 还有一个特别之处，还可以根据数据包的内容的值来过滤。

1.2 Filter 类型

HiPER 可提供三种基本的 Filter 类型：IP Filter，IPSSG Filter 和 Generic Filter。

1.2.1 IP Filter 介绍

IP Filter 只是对 IP 包进行判断和处理，其过滤依据主要是 IP 包头部信息，例如源 IP 地

址和目的 IP 地址。如果 IP 头中的协议字段封装协议为 TCP 或 UDP，则再根据 TCP 头信息（源端口和目的端口）或 UDP 头信息（源端口和目的端口）执行过滤。

1.2.2 IPSSG Filter 介绍

IPSSG Filter 是扩展的 Filter，是 HiPER 专有的 Filter。IPSSG Filter 的过滤依据除了 IP Filter 中的所有过滤依据之外，还包括 MAC 地址、时间段等信息。此外，IPSSG Filter 还实现了第七层过滤的功能，具体包括关键字过滤和 URL 过滤。

URL 过滤指对 URL 网址过滤，HiPER 的 URL 过滤功能是根据 URL 中的关键字进行过滤的，不仅可以控制局域网用户对站点的访问，还可以控制用户对网页的访问。

关键字过滤指对 HTML 页面（网页）中的关键字过滤，它的意思是如果某个网页里包含了你定义的关键字（如色情、法轮功、赌博等），那么 HiPER 将直接屏蔽这个网页。

1.2.3 Generic Filter 介绍

Generic Filter 是按照字节（bytes）或者比特（bits）检查任意类型的数据包。使用 Generic Filter，管理员需要知道数据包中所需匹配的某些字节的具体内容，比如说，某几个字节表示协议，那么就可以根据这几个字节在数据包中的位置、长度及其数值来设置 Filter 策略，从而检查数据包是否匹配。

1.2.4 三种类型比较

上述三种类型中，Generic Filter 执行效率最高，IP Filter 执行效率其次，IPSSG Filter 的效率最低。

IPSSG Filter 是在 IP Filter 基础上的扩充：IP Filter 具备的功能，IPSSG Filter 均具备。但是 IPSSG Filter 支持 MAC 地址过滤、时间段过滤、关键字过滤和 URL 过滤，IP Filter 不支持。因此，考虑到执行效率，当需要配置的 Filter 策略不涉及到 MAC 地址、时间段、第七层过滤等信息时，建议使用 IP Filter。当然，若涉及到这些信息，则需使用 IPSSG Filter。

Generic 主要用于 IP 协议之外的访问控制，如对使用 IPX、NETBIOS 等协议的控制；还可用于对应用程序的控制，如 QQ、MSN 等。

需要注意的是，HiPER 系列产品均支持 IP Filter 和 Generic Filter。业务管理系列产品均支持 IPSSG 功能，请查看相关产品的规格说明书。另外，还可使用 **revision** 命令查看，如果输出结果“ Feature enabled ”中包含 IPSSG 功能，则表示该产品可以使用 IPSSG Filter，下面给出一个例子（如图 1-1 所示）。

```
hiper% revision

loadname iv3300VFv501.bin 06:14:56PM-050317 hwu@entest.
MBID: 5100002
Feature enabled:   RTC   PPPOE   VPN   IPSSG   DMZ   CBQ
Product ID: 3300VF
```

表示该产品支持IPSSG Filter

图 1-1 使用 revision 命令查看是否支持 IP Filter

1.3 Filter 动作

Filter 的动作包括转发和丢弃，在 HiPER 中分别用“ forward=Yes ”和“ forward=No ”来表示。当需要处理的数据包与已定义的某条 Filter 策略相匹配时，如果该策略所定义的动作是转发，那么 HiPER 将转发该数据包；如果该策略所定义的动作是丢弃，那么 HiPER 将丢弃该数据包。

1.4 Filer 方向

Filter 的方向包括进入和外出，在 HiPER 中分别用“ In ”和“ Out ”来表示，Filter 方向用来指出是在数据包进入或离开 HiPER 时对其进行过滤。Filter 的方向与数据流方向、及其应用端口（物理端口或虚端口）密切相关，它们的涵义如下：

进入（In）— 当数据包从指定端口进入 HiPER 时执行过滤。数据包来自与指定端口相连的网络，希望穿过 HiPER 到达另一端口并转发。当指定端口接收到数据包之后，将首先进行 Filter 策略的匹配检查，如果有匹配策略，且该策略定义的动作是转发，那么将对该数据包进行路由处理；否则将直接丢弃该数据包。

外出（Out）— 当数据包从指定端口离开 HiPER 时执行过滤。数据包来自与另一端口相连的网络，已经穿过 HiPER 到达指定端口，并希望从该端口转发。当指定端口接收到数据包之后，将进行 Filter 策略的匹配检查，并根据匹配策略定义的动作处理该数据包：转发或丢弃。

以下将通过两个实例来说明 Filter 方向与数据流方向、以及应用端口的关系，如图 1-2、1-3 所示。图 1-2、1-3 中，都是通过 HiPER 连接两个网络：网络 A 和网络 B，其中，LAN 口连接到网络 A，WAN 口连接到网络 B。

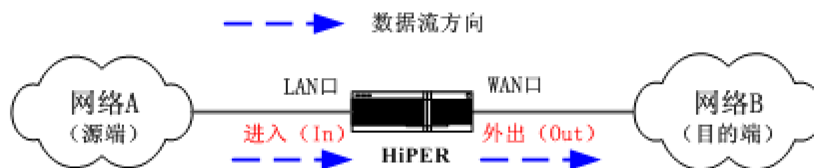


图 1-2 Filter 方向示意图 1

如图 1-2 所示，如果要求过滤从网络 A 发起经过 HiPER 转发到网络 B 的流量，那么，从 HiPER 的 LAN 口来看，是接收到数据包；而从 WAN 口来看，则是发送数据包。因此，

当在 LAN 口启用 Filter 功能时，其方向需定义为 In；当在 WAN 口启用 Filter 功能时，其方向需定义为 Out。

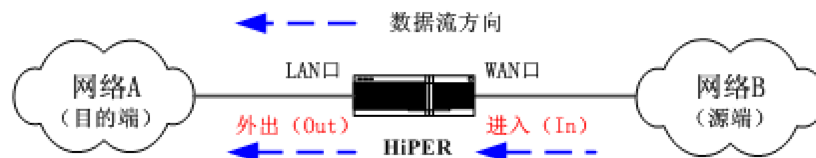


图 1-3 Filter 方向示意图 2

如图 1-3 所示，如果要求过滤从网络 B 发起经过 HiPER 转发到网络 A 的流量，那么，从 HiPER 的 WAN 口来看，是接收到数据包；而从 LAN 口来看，则是发送数据包。因此，当在 WAN 口启用 Filter 功能时，其方向需定义为 In；当在 LAN 口启用 Filter 功能时，其方向需定义为 Out。

由上可以看出，Filter 方向为 In 或 Out，将导致在 HiPER 内部是先进行路由处理还是先进行 Filter 匹配检查。Filter 方向为 In 时，HiPER 将首先进行 Filter 策略的匹配检查，再进行路由处理。Filter 方向为 Out 时，HiPER 是先进行路由处理选择外出接口，再在该接口进行 Filter 策略的匹配检查。因此，一般情况下，为了提高 HiPER 的效率，避免对将被丢弃的数据包进行路由处理，建议将 Filter 应用于与数据包源端所在网络相连（靠近）的接口，此时 Filter 方向为 In。

提示：

1. 一般情况下，由于 HiPER 会启用 NAT 功能，所有的局域网计算机将仅使用一个或几个公网地址连接到 Internet，因此，通常都是过滤从企业内部局域网到 Internet 的流量。同时，由于一般都是 LAN 口接局域网，因此通常都是在 LAN 口启用 Filter，其方向为 In。
2. 此外，HiPER 也支持在拨号虚端口（比如 PPPoE、L2TP/PPTP 拨号虚端口）启用 Filter 功能，在本手册中也将做相关介绍。

1.5 Filter 工作原理

当 HiPER 上没有启用 Filter 功能时，HiPER 收到没有错误的可路由的数据包，会直接根据路由表转发到相应的接口，并发送到下一跳。当定义了 Filter 策略并在某个端口启用 Filter 功能，HiPER 将会检查该端口收到或发出的每一个数据包，判断是否有符合的 Filter 策略。

所有的 Filter 策略也将按照配置的顺序依次存放在策略表中，任何后续的增加部分都放入策略表的底部。当数据包到达 HiPER 的指定端口后，HiPER 将从策略表的顶端从上至下搜索策略列表，查找是否有匹配策略，并执行匹配的第一个策略。具体地说，当配置了多个 Filter 策略时，HiPER 在指定的接口收到或者发出一个数据包时，将首先去同 Filter 策略表中的第一个策略比较，如果不匹配，那么将去同第二个策略比较，……，依此类推，一直到匹配成功为止。如果其中的一个匹配成功，那么就执行该策略定义的动作：转发或丢弃，并且，不再继续比较其余的策略。如果与所有的 Filter 策略都不能匹配，处于安全的考虑，HiPER 将丢弃这个数据包。

Filter 策略定义前后之间是无关的，如果第一个定义的动作是转发，第二个可以是丢弃，

第三个可以是转发，等等。但是由于 HiPER 将会对数据包执行第一个匹配的策略所定义的动作，因此，必须按照从特殊到一般的顺序安排、配置策略。特殊策略不排除位于列表下部的更一般性策略的应用，但位于特殊策略前的一般性策略会产生此排除效应。举个例子来说，要求禁止局域网用户使用 MSN 业务，允许其他所有业务。那么就需要先配置禁止 MSN 业务的策略，再配置允许所有业务的策略。

1.6 Filter 分组

HiPER 中，Filter 策略还支持分组功能，当需要多个业务策略用在不同的地方时，就可以使用分组功能。分组功能是通过为业务策略设置 **groupname**（组名）来实现的，方向相同、组名相同的业务策略划分在同一个业务策略组中。

另外，方向为 In、未定义组名的业务策略全部都划分在同一个业务策略组中，称为业务策略缺省组 In；方向为 Out、未定义组名的业务策略也全部都划分在同一个业务策略组中，称为业务策略缺省组 Out。

对于每一个端口来说，在进入（In）或者外出（Out）方向上可以设置不同的业务策略组，但是，一个方向同时只能设置一个业务策略组。如果在某个端口启用了某个方向为 In 的业务策略组，那么，该组中的业务策略将作用于从该端口进入 HiPER 的数据包；如果在某个端口启用了某个方向为 Out 的业务策略组，那么，该组中的业务策略将作用于从该端口离开 HiPER 的数据包。

注意，如果某个端口未设置所启用的业务策略组，那么，系统业务策略缺省组中的业务策略（即未定义组名的业务策略）将作用于该端口。

第2章 业务策略配置

2.1 业务策略配置

如章节 1.2 中所述，HiPER 提供三种类型的业务策略：IP Filter、IPSSG Filter 以及 Generic Filter。虽然这三种类型的业务策略的配置方法各自不同，但是，业务策略配置中有某些命令是与 Filter 类型无关的，因此，以下各节将首先介绍这些与 Filter 类型无关的基本配置，再分别介绍这三种类型的业务策略的配置方法及注意事项。

2.1.1 基本配置

本节主要介绍与 Filter 类型无关的一些基本配置命令，也就是说，它们适用于任何一种类型的业务策略。主要内容如下：

- 新建一条业务策略
- 设置业务策略的类型
- 设置业务策略的动作
- 设置业务策略的组名
- 启用/禁用一条业务策略
- 删除一条业务策略

2.1.1.1 新建一条业务策略

首先需要创建一条业务策略，并为该业务策略自定义一个名称。注意，同时还需指定该业务策略的方向。在对该业务策略进行其他配置时，必须使用相同的方向。

配置命令如表 2-1 所示。

操作	命令
新建一条业务策略	**new filter** {**in** | **out**}/*filter-name*
备注：*filter-name* 为用户自定义的业务策略的名称； **in** 表示过滤方向为进入，即对从指定端口进入 HiPER 的数据包进行过滤； **out** 表示过滤方向为外出，即对从指定端口离开 HiPER 的数据包进行过滤。	

表 2-1 新建一条业务策略——IP Filter

2.1.1.2 设置业务策略的类型

如章节 1.2 中所述，HiPER 支持 3 种类型的业务策略：IP Filter、IPSSG Filter 以及 Generic Filter。缺省情况下，业务策略的类型为 Generic。

配置命令如表 2-2 所示。

操作	命令
设置业务策略的类型为 IP Filter	**set filter** {**in** | **out**}/*filter-name* **type { ip | ipssg| generic}**
备注：**type** 的缺省值为 **generic**。	

表 2-2 设置业务策略的类型

2.1.1.3 设置业务策略的动作

如章节 1.3 中所述，业务策略的动作包括转发和丢弃。

配置命令如表 2-3 所示。

操作	命令
设置业务策略的动作	**set filter** {**in** | **out**}/*filter-name* **forward {yes | no}**
备注：**yes** 表示允许，与此策略匹配的数据包将被转发，为缺省值； **no** 表示禁止，与此策略匹配的数据包将被丢弃。	

表 2-3 设置业务策略的动作

2.1.1.4 设置业务策略的组名

如章节 1.6 中所述，业务策略还支持分组功能，当需要多个业务策略用在不同的地方时，就可以使用分组功能。

业务策略的分组功能是通过设置业务策略的 **groupname**（组名）来实现的，方向相同、组名相同的业务策略划分在同一个业务策略组中。

另外，方向为 In、未定义组名的业务策略全部都划分在同一个组中，称为业务策略缺省组 In；方向为 Out、未定义组名的业务策略也全部都划分在同一个组中，称为业务策略缺省组 Out。

配置命令如表 2-4 所示。

操作	命令
设置业务策略的组名	**set filter** {**in** | **out**}/*filter-name* **groupname** *filter-groupname*
备注：**groupname** 的缺省值为空。	

表 2-4 设置业务策略的组名

2.1.1.5 启用/禁用一条业务策略

允许设置各条业务策略的使能状态：启用或禁用。如果你暂时不需要使用某条业务策略，只需禁用它即可，此时该业务策略仅在配置文件中可见，但不再有效；当需要恢复使用该业务策略时，只需启用它即可。

配置命令如表 2-5 所示。

操作	命令
启用一条业务策略	**set filter** {**in** | **out**}/*filter-name* **enabled yes**
禁用一条业务策略	**set filter** {**in** | **out**}/*filter-name* **enabled no**
备注：缺省情况下，为启用业务策略。	

表 2-5 启用/禁用一条业务策略

2.1.1.6 删除一条业务策略

如有需要，可删除已配置的业务策略，一次只能删除一条。

配置命令如表 2-6 所示。

操作	命令
删除一条业务策略	**delete filter** {**in** | **out**}/*filter-name*
备注：删除某条业务策略时，输入的 *filter -name* 必须与新建该业务策略时输入的名字全字匹配。	

表 2-6 删除一条业务策略

2.1.2 业务策略配置——IPSSG Filter

除章节 2.1.1 中介绍的基本配置外，IPSSG Filter 策略的配置主要还包括以下内容：

- 设置 IPSSG Filter 的源/目的 IP 地址
- 设置 IPSSG Filter 的协议类型
- 设置 IPSSG Filter 的源/目的端口
- 设置 IPSSG Filter 的生效时间段
- 设置 IPSSG Filter 的源/目的 MAC 地址
- 设置 IPSSG Filter 的以太网类型
- 设置业 IPSSG Filter 的 TCP 连接方向
- 设置 IPSSG Filter 的第七层过滤功能

2.1.2.1 设置 IPSSG Filter 的源/目的 IP 地址

对于 IPSSG Filter 来说，可通过两种方式设置业务策略的源/目的 IP 地址，一种方式是通过设置源/目的起始 IP 地址和结束 IP 地址实现，另外一种方式是通过设置源/目的 IP 地址及其子网掩码来实现，以下将分别说明。

注意，ReOS 460（含 460）以上版本才支持方式 1。另外，每次只允许选择其中的一种方式来设置源/目的 IP 地址，请不要同时使用两种方式。

1. 方式 1

本方式下，通过设置参数 **srcfrom**（源起始 IP 地址）和 **srcend**（源结束 IP 地址）过滤源 IP 地址；通过设置参数 **destfrom**（目的起始 IP 地址）和 **destend**（目的结束 IP 地址）过滤的目的 IP 地址。

配置命令如表 2-7 所示。

操作	命令
设置 IPSSG Filter 的源起始 IP 地址	**set filter** {**in** | **out**}/*filter-name* **ipssg srcfrom** *srcfrom*
设置 IPSSG Filter 的源结束 IP 地址	**set filter** {**in** | **out**}/*filter-name* **ipssg srcend** *srcend*
设置 IPSSG Filter 的目的起始 IP 地址	**set filter** {**in** | **out**}/*filter-name* **ipssg destfrom** *destfrom*
设置 IPSSG Filter 的目的结束 IP 地址	**set filter** {**in** | **out**}/*filter-name* **ipssg destend** *destend*
备注：缺省情况下，**srcfrom**、**srcend**、**destfrom** 和 **destend** 的值都为 0.0.0.0。	

表 2-7 设置 IPSSG Filter 的源/目的 IP 地址——方式 1

本方式下，过滤源 IP 地址和过滤目的 IP 地址的方法类似，这里以如何过滤目的 IP 地址为例进行说明：

1) 如果要过滤单个地址，则需将 **destfrom** 和 **destend** 均设为预指定的 IP 地址；

2) 如果要过滤一段范围的 IP 地址，则需将 **destfrom** 设为这段地址的起始地址，将 **destend** 设为这段地址的结束地址。例如如果某策略需要过滤的源 IP 地址范围为 218.1.1.2～218.1.1.5，则需将 **destfrom** 和 **destend** 分别设为 218.1.1.2、218.1.1.5。

3) 缺省情况下，**destfrom** 和 **destend** 的值都为 0.0.0.0，表示不限制目的 IP 地址。

2. 方式 2

本方式下，通过设置参数 **srcaddr**（源 IP 地址）和 **srcmask**（源 IP 掩码）过滤源 IP 地址；通过设置参数 **destaddr**（目的 IP 地址）和 **destmask**（目的 IP 掩码）过滤目的 IP 地址。

配置命令如表 2-8 所示。

操作	命令
设置 IPSSG Filter 的源 IP 地址	**set filter** {**in** | **out**}/*filter-name* **ipssg srcaddr** *srcaddr*
设置 IPSSG Filter 的源 IP 掩码	**set filter** {**in** | **out**}/*filter-name* **ipssg srcmask** *srcmask*
设置 IPSSG Filter 的目的 IP 地址	**set filter** {**in** | **out**}/*filter-name* **ipssg destaddr** *destaddr*
设置 IPSSG Filter 的目的 IP 掩码	**set filter** {**in** | **out**}/*filter-name* **ipssg destmask** *destmask*
备注：缺省情况下，**srcaddr**、**srcmask**、**destaddr** 与 **destmask** 的值都为 0.0.0.0。	

表 2-8 设置 IPSSG Filter 的源/目的 IP 地址——方式 2

本方式下，过滤源 IP 地址和过滤目的地址的方法类似，这里以如何过滤源 IP 地址为例进行说明：

1) 如果要配置单机用户，则需将 **srcmask** 设为 255.255.255.255，**srcaddr** 为该主机的 IP 地址；

2) 如果要配置一段范围的源 IP 地址，则需将 **srcmask** 设为这段地址的子网掩码，

srcaddr 为该范围内任意一个 IP 地址。例如如果某策略的源 IP 地址范围为 192.168.1.1～192.168.1.31，则需将 **srcmask** 设为 255.255.255.224；

3) 缺省情况下，**srcaddr** 和 **srcmask** 的值都为 0.0.0.0，表示不限制源 IP 地址。

2.1.2.2 设置 IPSSG Filter 的协议类型

对于 IPSSG Filter 来说，数据包的协议类型可用数字表示（附录一列举了常用的 IP 协议号），如：UDP 为 17，TCP 为 6。此外，以下协议可以直接输入协议名：AH、ESP、GRE、ICMP、IGMP、IPIP（IPINIP 的简称）、OSPF、TCP、UDP。其中，缺省值为 any，表示任意协议；另外，0 也可用来表示任意协议。

配置命令如表 2-9 所示。

操作	命令
设置 IPSSG Filter 的协议类型	**set filter** {**in** | **out**}/*filter-name* **ipssg protocol** *protocol*
备注：缺省情况下，**protocol** 的值为 **any**，表示任意协议。	

表 2-9 设置 IPSSG Filter 的协议类型

注意，只有在指定协议类型为“ TCP ”或“ UDP ”之后，源（目的）端口的相关配置才有效。如果将协议类型设置为“ 0 ”或“ any ”(表示任意协议)，那么将无法取到包的端口信息，从而所有端口设置将被忽略。协议类型设置为“ TCP ”或“ UDP ”时，如果不指定源端口或目的端口，则表示 TCP/UDP 报文的所有源端口或目的端口信息都匹配。

2.1.2.3 设置 IPSSG Filter 的源/目的端口

对于 IPSSG Filter 来说，可通过两种方式设置业务策略的源/目的端口，一种方式是通过设置源/目的起始端口和结束端口实现，另外一种方式是通过设置源/目的端口和端口匹配动作来实现，以下将分别说明。

注意，ReOS 460（含 460）以上版本才支持方式 1。另外，每次只允许选择其中的一种方式来设置源/目的 IP 地址，请不要同时使用两种方式。

此外，如章节 2.1.2.2 中所述，只有在指定的 **protocol**（协议类型）是“ TCP ”或“ UDP ”之后，源（目的）端口的相关配置才有效；附录二提供了常用 TCP/UDP 端口号。

1. 方式 1

本方式下，通过设置参数 **sportfrom**（源起始端口）和 **sportend**（源结束端口）过滤源端口；通过设置参数 **dportfrom**（目的起始端口）和 **dportend**（目的结束端口）过滤目的端口。

配置命令如表 2-10 所示。

操作	命令
设置 IPSSG Filter 的源起始端口	**set filter** {**in** | **out**}/*filter-name* **ipssg sportfrom** *sportfrom*
设置 IPSSG Filter 的源结束端口	**set filter** {**in** | **out**}/*filter-name* **ipssg sportend** *sportend*

设置 IPSSG Filter 的目的起始端口	**set filter** {**in** | **out**}/*filter-name* **ipssg dportfrom** *dportfrom*
设置 IPSSG Filter 的目的结束端口	**set filter** {**in** | **out**}/*filter-name* **ipssg dportend** *dportend*
备注：缺省情况下，**sportfrom**、**sportend**、**dportfrom** 和 **dportend** 的值都为 0。	

表 2-10 设置 IPSSG Filter 的源/目的端口——方式 1

本方式下，过滤源端口和过滤目的端口的方法类似，这里以如何过滤目的端口为例进行说明：

1) 如果要过滤单个目的端口，则需将 **dportfrom** 和 **dportend** 均设为预指定的端口。
2) 过滤一段范围的目的端口，有以下三种情况：
   a) 如果要过滤某段范围内的端口（包括起始端口和结束端口），则需将 **dportfrom** 设为起始端口，将 **dportend** 设为结束端口。
   b) 如果要过滤的端口范围为大于某个指定端口号的所有端口（包括该指定端口），则需将 **dportfrom** 设为指定端口，并将 **dportend** 设为 **65535**。
   c) 如果要过滤的端口范围为小于某个指定端口的所有端口（包括该指定端口），则需将 **dportfrom** 设为 0，并将 **dportend** 设为指定端口。
3) 缺省情况下，**dportfrom** 和 **dportend** 的值都为 0，表示不限制目的端口。

2. 方式 2

本方式下，通过设置参数 **srcport**（源端口）和 **srcportcmp**（源端口匹配动作）过滤源端口；通过设置参数 **destport**（目的端口）和 **destportcmp**（目的端口匹配动作）过滤的目的端口。

配置命令如表 2-11 所示。

操作	命令
设置 IPSSG Filter 的源端口	**set filter** {**in** | **out**}/*filter-name* **ipssg srcport** *srcport*
设置 IPSSG Filter 的源端口匹配动作	**set filter** {**in** | **out**}/*filter-name* **ipssg srcportcmp { none** | **less** | **eql** | **gtr** | **neq}**
设置 IPSSG Filter 的目的端口	**set filter** {**in** | **out**}/*filter-name* **ipssg destport** *destport*
设置 IPSSG Filter 的目的端口匹配动作	**set filter** {**in** | **out**}/*filter-name* **ipssg destportcmp { none** | **less** | **eql** | **gtr** | **neq}**
备注：缺省情况下，**srcport** 值为 0， 表示不限制源端口；**destport** 值为 0，表示不限制目的端口；**srcportcmp** 和 **destportcmp** 值都为 **none**，表示无动作。	

表 2-11 设置 IPSSG Filter 的源/目的端口——方式 2

本方式下，过滤源端口和目的端口的方法类似，这里以如何过滤源端口为例进行说明：

1) 如果要配置单个端口，只需将 **srcport** 设置为指定端口号，将 **srcportcmp** 设为 **eql**（即等于）即可。
2) 配置一段范围的端口，有以下三种情况：
   a) 如果要配置的端口范围为大于某个端口号的所有端口，只需将 **srcport** 设置为指定端口号，并将 **srcportcmp** 设为 **gtr**（即大于）即可。
   b) 如果要配置的端口范围为小于某个端口的所有端口，只需将 **srcport** 设置为指

定端口号，并将 **srcportcmp** 设为 **less**（即小于）即可。

c) 如果要配置某段范围内的端口，则需要通过配置两个策略实现，即将上述 b、c 所述结合起来使用。

3) 缺省情况下，**srcport** 的值为 0，表示不限制源端口。

2.1.2.4 设置 IPSSG Filter 的生效时间段

对于 IPSSG Filter 来说，可以设置业务策略的生效时间段。一旦指定了生效时间段，则表示该策略仅仅在指定的时间段范围内有效。缺省情况下，为不指定生效时间段，表示该策略不受时间限制。

配置命令如表 2-12 所示。

操作	命令
设置 IPSSG Filter 的生效时间段	**set filter** {**in** | **out**}/*filter-name* **ipssg timerange** *time-name*
备注：缺省情况下，**timerange** 的值为空，表示不指定生效时间段。	

表 2-12 设置 IPSSG Filter 的协议类型

提示：“ *time-name* ”为业务策略的生效时间段的实例名，时间段的配置方法请参考手册《HiPER 命令行配置手册 第 2 卷：基本配置》的第 4 章（时间段配置），这里不再介绍。

2.1.2.5 设置 IPSSG Filter 的源/目的 MAC 地址

对于 IPSSG Filter 来说，通过设置参数 **smac**（源 MAC 地址）和 **sneq**（源 MAC 地址比较符）过滤源 MAC 地址；通过设置参数 **dmac**（目的 MAC 地址）和 **dneq**（目的 MAC 地址比较符）过滤目的 MAC 地址。

配置命令如表 2-13 所示。

操作	命令
设置 IPSSG Filter 的源 MAC 地址	**set filter** {**in** | **out**}/*filter-name* **ipssg smac** *smac*
设置 IPSSG Filter 的源 MAC 地址比较符	**set filter** {**in** | **out**}/*filter-name* **ipssg sneq** {**equals** | **notequals**}
设置 IPSSG Filter 的目的 MAC 地址	**set filter** {**in** | **out**}/*filter-name* **ipssg dmac** *dmac*
设置 IPSSG Filter 的目的 MAC 地址比较符	**set filter** {**in** | **out**}/*filter-name* **ipssg dneq** {**equals** | **notequals**}
备注：缺省情况下，**smac** 和 **dmac** 的值都为 **000000000000**；**sneq** 和 “ **dneq** ” 的值都为 **equals**。	

表 2-13 设置 IPSSG Filter 的源/目的 MAC 地址

实际应用中，过滤源 MAC 地址和过滤目的 MAC 地址的方法类似，这里以过滤源 MAC 地址为例进行说明。

1) 当 **sneq** 为 **equals** 时，表示数据包的源 MAC 地址与指定 MAC 地址相等时匹配；

2) 当 **sneq** 为 **notequals** 时，表示数据包的源 MAC 地址与指定 MAC 地址不相等时匹配。

⌖提示：ReOS 4.4 以上版本中，由于用户管理（IP/MAC 绑定）功能也支持过滤源 MAC 地址，且执行效率更高，因此，如果仅需要过滤源 MAC 地址，建议使用 IP/MAC 绑定功能。IP/MAC 绑定功能的具体配置方法请参考手册《HiPER 命令行配置手册 第 3 卷：网络层协议》的章节 1.3.1 和章节 1.3.2。

2.1.2.6 设置 IPSSG Filter 的以太网类型

对于 IPSSG Filter 来说，可通过配置参数 **etype**（以太网类型）和 **eneq**（以太网类型比较符）来限制以太网类型，这两个参数的取值如下所述：

etype：输入方式有两种，一种是输入以太网类型的代码，取值范围：0~65535，10 进制方式输入；缺省值为 0，代表不检查以太网类型。另一种是输入代表以太网类型的一般字符串，只有以下几种以太网类型支持该方式：ip、arp、rarp、addp、aarp、ipx、pppoed、pppoes。

eneq：枚举型参数，**eneq** 设置为 **equals** 时，表示以太网类型和预先设置的类型相同时匹配；**eneq** 设置为 **notequals** 时，表示以太网类型和预先设置的类型不同时匹配。

配置命令如表 2-14 所示。

操作	命令
设置 IPSSG Filter 的以太网类型	**set filter** {**in** | **out**}/*filter-name* **ipssg etype** *etype*
设置 IPSSG Filter 的以太网类型比较符	**set filter** {**in** | **out**}/*filter-name* **ipssg eneq** {**equals** | **notequals**}
备注：缺省情况下，**etype** 的值为 0，表示不检查以太网类型；**sneq** 的值为 **equals**。	

表 2-14 设置 IPSSG Filter 的以太网类型

2.1.2.7 设置 IPSSG Filter 的 TCP 连接方向

对于 IPSSG Filter 来说，可通过配置参数 **tcpestab**（TCP 连接方向）实现 TCP 单向访问连接，即只允许已经建立了 TCP 连接的报文通过，初始化连接报文被拒绝，这样可以增加业务策略的安全性。如果 TCP 报文中设置了应答位（ACK）和复位位（RST），则表示该报文为已经建立的 TCP 连接报文。

一般情况下，无需限制 TCP 连接方向。但是，当 HiPER 未启用 NAT 功能时，如果需要实现 TCP 单向访问连接，比如希望某个 TCP 连接只能由局域网主机发起，禁止 Internet 上的主机主动发起建立连接请求，就需要限制 TCP 连接方向。注意，这种情况下，需过滤从 Internet 到局域网的流量。

配置命令如表 2-15 所示。

操作	命令
设置 IPSSG Filter 限制 TCP 连接方向	**set filter** {**in** | **out**}/*filter-name* **ipssg tcpestab yes**
设置 IPSSG Filter 不限制 TCP 连接方向	**set filter** {**in** | **out**}/*filter-name* **ipssg tcpestab no**
备注：缺省情况下，为不限制 TCP 连接方向。	

表 2-15 设置 IPSSG Filter 的 TCP 连接方向

2.1.2.8 设置 IPSSG Filter 的第七层过滤功能

如章节 1.2.2 中所述，IPSSG Filter 还支持第七层过滤功能，包括：URL 过滤和关键字过滤。缺省情况下，不启用第七层过滤功能。

URL 过滤指对 URL 网址过滤，HiPER 的 URL 过滤功能是根据 URL 中的关键字进行过滤的，当访问的网页的 URL 中含有与 " 过滤内容 " 完全匹配的字段时，就认为是匹配该策略的。这样，不仅可以控制局域网用户对站点的访问，还可以控制用户对网页的访问。

关键字过滤指对 HTML 页面（网页）中的关键字过滤，它的意思是如果某个网页里包含了你定义的关键字（如色情、法轮功、赌博等），那么 HiPER 将直接屏蔽这个网页。CLI 中，HiPER 的关键字过滤功能仅支持英文关键字的设置。

配置命令如表 2-16 所示。

操作	命令
设置 IPSSG Filter 的过滤类型	**set filter** {**in** | **out**}/*filter-name* **ipssg L7filter** {**alg_none** | **url_alg** | **str_alg** }
设置 IPSSG Filter 的过滤内容	**set filter** {**in** | **out**}/*filter-name* **ipssg L7key** *L7key*
备注：缺省情况下，**L7filter** 值为 **alg_none**，表示不启用第七层过滤功能；**L7key** 的值为空。	

表 2-16 设置 IPSSG Filter 的第七层过滤功能

实际应用中，第七层过滤功能的配置方法及注意事项如下：

1) 为方便起见，一般建议使用 WEB UI 设置第七层过滤功能。

2) 缺省情况下，参数 **L7filter**（过滤类型）的值为 **alg_none**，表示不启用第七层过滤功能。如果需要启用 URL 过滤功能，则需将 **L7filter** 设置为 **url_alg**；如果需要启用关键字过滤功能，则需将 **L7filter** 设置为 **str_alg**。

3) 目前，启用 URL 过滤或者关键字过滤功能时，必须将相关 IPSSG Filter 的协议类型设置为 TCP（章节 2.1.2.2），并且将目的端口设置为 80（章节 2.1.2.3）。这两种情况下，可能需要设置源地址、生效时间段等，但是，一般无需设置目的 IP 地址和源端口。

4) 启用 URL 过滤功能时，参数 **L7key**（过滤内容）可以是一个完整的域名，这时，该域名开头的所有网页都被匹配；也可输入域名的子字符串，这时，URL 中包含该子字符串的所有网页都被匹配，从而实现对某个站点的所有网页的过滤。输入 URL 时，请不要包含 http://；URL 地址中，英文字符不区分大小写。

为方便理解，下面举几个例子进行说明：

例 1，如果输入 www.sina.com.cn，那么以 www.sina.com.cn 开头的所有网页都将匹配该策略，如 www.sina.com.cn/index.jsp，但是 tech.sina.com.cn 开头的网页却不被匹配。

例 2，如果输入 www.utt.com.cn/bbs/，则以 www.utt.com.cn/bbs/ 开头的所有网页都将匹配该策略，从而控制对 utt 这个站点中 bbs 页面的访问。

例 3，如果输入 sina.com，那么所有出现 sina.com 和 sina.com.cn 的网页都被匹配，相当于整个 sina 站点都被匹配，当然，此时以 tech.sina.com.cn 开头的网页将被匹配。

5) 目前，CLI 中启用关键字过滤功能时，参数 **L7key**（过滤内容）仅支持英文输入方式，取值范围：1~31 个字符。

6) 参数 **L7key**（过滤内容）中，不支持使用通配符 " * " 或者 " ? " 来代表任意字符。

2.1.3 业务策略配置——IP Filter

除章节 2.1.1 中介绍的基本配置外，IP Filter 策略的配置主要还包括以下内容：

- 设置 IP Filter 的源/目的 IP 地址
- 设置 IP Filter 的协议类型
- 设置 IP Filter 的源端口和目的端口
- 设置 IP Filter 的的 TCP 连接方向

2.1.3.1 设置 IP Filter 的源/目的 IP 地址

与 IPSSG Filter 不同，IP Filter 仅支持一种方式设置源/目的 IP 地址，即通过设置源/目的 IP 地址及其子网掩码来实现。IP Filter 中，过滤源/目的 IP 地址的配置方法与 IPSSG Filter 中的相关配置方法类似，具体请参考章节 2.1.2.1 的方式 2 中的相关描述。注意，二者的配置命令略有不同。

配置方法如表 2-17 所示。

操作	命令
设置 IP Filter 的源 IP 地址	**set filter** {**in** | **out**}/*filter-name* **ip srcaddr** *srcaddr*
设置 IP Filter 的源 IP 掩码	**set filter** {**in** | **out**}/*filter-name* **ip srcmask** *srcmask*
设置 IP Filter 的目的 IP 地址	**set filter** {**in** | **out**}/*filter-name* **ip destaddr** *destaddr*
设置 IP Filter 的目的 IP 掩码	**set filter** {**in** | **out**}/*filter-name* **ip destmask** *destmask*
备注：缺省情况下，**srcaddr**、**srcmask**、**destaddr** 与 **destmask** 的值都为 0.0.0.0。	

表 2-17 设置 IP Filter 的源/目的 IP 地址

2.1.3.2 设置 IP Filter 的协议类型

与 IPSSG Filter 不同，IP Filter 中数据包的协议类型只能用数字表示（附录一列举了常用的 IP 协议号），如：UDP 为 17，TCP 为 6。缺省值为 0，表示任意协议。

配置命令如表 2-18 所示。

操作	命令
设置 IP Filter 的协议类型	**set filter** {**in** | **out**}/*filter-name* **ip protocol** *protocol*
备注：缺省情况下，**protocol** 的值为 **any**，表示任意协议。	

表 2-18 设置 IP Filter 的协议类型

注意，只有在指定协议类型为“6（TCP）”或“17（UDP）”之后，源（目的）端口的相关配置才有效。如果将协议类型设置为“0”(表示任意协议)，那么将无法取到包的端口信息，从而所有端口设置将被忽略。协议类型设置为“TCP”或“UDP”时，如果不指定源端口或目的端口，则表示 TCP/UDP 报文的所有源端口或目的端口信息都匹配。

2.1.3.3 设置 IP Filter 的源/目的端口

与 IPSSG Filter 不同，IP Filter 仅支持一种方式设置源/目的 IP 地址，即通过设置源/目的端口和端口匹配动作来实现。IP Filter 中，过滤源/目的 IP 地址的配置方法与 IPSSG Filter 中的相关配置方法类似，具体请参考章节 2.1.2.3 的方式 2 中的相关描述。注意，二者的配置命令略有不同。

配置命令如表 2-19 所示。

操作	命令
设置 IP Filter 的源端口	**set filter** {**in** | **out**}/*filter-name* **ip srcport** *srcport*
设置 IP Filter 的源端口匹配动作	**set filter** {**in** | **out**}/*filter-name* **ip srcportcmp { none | less | eql | gtr | neq}**
设置 IP Filter 的目的端口	**set filter** {**in** | **out**}/*filter-name* **ip destport** *destport*
设置 IP Filter 的目的端口匹配动作	**set filter** {**in** | **out**}/*filter-name* **ip destportcmp { none | less | eql | gtr | neq}**
备注：缺省情况下，**srcport** 值为 0， 表示不限制源端口； **destport** 值为 0，表示不限制目的端口；**srcportcmp** 和 **destportcmp** 值都为 **none**，表示无动作。	

表 2-19 设置 IP Filter 的源/目的端口

2.1.3.4 设置 IP Filter 的 TCP 连接方向

与 IPSSG Filter 一样，IP Filter 也支持实现 TCP 单向访问控制，二者的相关应用及配置方法类似，具体描述请参考章节 2.1.2.7。注意，二者的配置命令略有不同。

配置命令如表 2-20 所示。

操作	命令
设置 IP Filter 限制 TCP 连接方向	**set filter** {**in** | **out**}/*filter-name* **ip tcpestab yes**
设置 IP Filter 不限制 TCP 连接方向	**set filter** {**in** | **out**}/*filter-name* **ip tcpestab no**
备注：缺省情况下，为不限制 TCP 连接方向。	

表 2-20 设置 IP Filter 的 TCP 连接方向

2.1.4 业务策略配置——Generic Filter

除章节 2.1.1 中介绍的基本配置外，Generic Filter 策略的配置主要还包括以下内容：

- 设置 Generic Filter 的比较内容
- 设置 Generic Filter 的匹配值及其匹配动作
- 设置是否需要连续检查后续的 Genererci Filter

2.1.4.1 设置 Generic Filter 的比较内容

Generic Filter 中，通过参数 **offset**（偏移量）、**length**（比较长度）以及 **mask**（匹配掩码）来设置数据包的比较内容。

配置命令如表 2-21 所示。

操作	命令
设置 Generic Filter 的偏移量	**set filter** {**in** | **out**}/*filter-name* **generic offset** *offset*
设置 Generic Filter 的比较长度	**set filter** {**in** | **out**}/*filter-name* **generic length** *length*
设置 Generic Filter 的匹配掩码	**set filter** {**in** | **out**}/*filter-name* **generic mask** *mask*
备注：**offset** 的缺省值为 **0**；取值范围：0-1510；单位：字节。 **length** 的缺省值为 **0**；取值范围：0-8；单位：字节。 **mask** 的缺省值为 **0000000000000000**；16 进制格式输入，取值范围：1~16 位。	

表 2-21 设置 Generic Filter 的偏移量

offset（偏移量）是指数据包需要比较的内容的起始位置距离包头（包括以太网包头）的字节数。例如，如果将 **offset** 设置为 34，则表示偏移量为 34 字节，即从第 35 个字节开始比较。

length（比较长度）是指数据包需要比较的内容的长度，也用字节数计算。例如，如果将 **length** 设置为 4，则表示一共需要比较 4 个字节。

由参数 **offset** 和 **length** 确定的数据称为原始比较数据，原始比较数据与 **mask** 相与（换成 2 进制计算）的结果就是数据包中实际要比较的内容。也就是说，原始比较数据中，**mask** 为 1（2 进制）对应的地址位需要严格匹配，而 **mask** 为 0（2 进制）对应的地址位则无需匹配。**mask** 使用 16 进制格式输入，取值范围 1~16 位；注意，系统中 **mask** 的值始终都为 16 位，当输入的值不足 16 位时，系统将会自动在低位填入 0。

2.1.4.2 设置 Generic Filter 的匹配值及其匹配动作

Generic Filter 中，通过参数 **value** 设置数据包中比较内容的匹配值，通过参数 **compare** 设置匹配动作。

配置命令如表 2-22 所示。

操作	命令
设置 Generic Filter 的匹配值	**set filter** {**in** | **out**}/*filter-name* **generic value** *value*
设置 Generic Filter 的匹配动作	**set filter** {**in** | **out**}/*filter-name* **generic compare** {**equals** | **notequals**}
备注：**value** 的缺省值为 **0000000000000000**；16 进制格式输入，取值范围：1~16 位。	

表 2-22 设置 Generic Filter 的匹配内容

与 **mask** 类似，**value** 使用 16 进制格式输入，取值范围 1~16 位；并且，**value** 和 **mask** 的位数必须相同。注意，系统中 **value** 的值始终都为 16 位，当输入的值不足 16 位时，系统

将会自动在低位填入 0。

参数 **value** 和 **compare** 需结合使用，具体描述如下：

1) 当 **compare** 设置为 **equals** 时，表示由 **offset**、**length** 以及 **mask** 计算出的比较内容（章节 2.1.4.1）与 **value** 的值相等时匹配。

2) 当 **compare** 设置为 **notequals** 时，表示由 **offset**、**length** 以及 **mask** 计算出的比较内容（章节 2.1.4.1）与 **value** 的值不等时匹配。

2.1.4.3 设置是否需要连续检查后续的 Generci Filter

由于对于每一个 Generic Filter 来说，数据包比较长度最多为 8 个字节（章节 2.1.4.2），因此，如果数据包中需要比较的内容的长度超过了 8 个字节，就需要通过设置多个 Generic Filter 实现，这些连续的策略构成一个大策略组。这时，需要将该组中的前面几条业务策略设置为需要连续检查后续策略（**more** 设置为 **yes**）；将该组中的最后一条策略设置为不需要连续检查后续策略（**more** 设置为 **no**），表示大策略组结束。检查数据包是否符合业务策略时，这个大策略组是作为一个整体的，也就是说，数据包的内容必须与这个大策略组中的所有策略都匹配，才认为是符合过滤条件的。

一般，当过滤条件要求同时检查数据包的几个不同地方时，就需要设置一组连续的相关策略来实现。例如，假设过滤条件为 UDP 1701 端口，就需要设置两个连续的业务策略，分别用来过滤 UDP 协议和 1701 端口，这两个业务策略就构成一个大策略组。该组中的第一个策略的 **more** 设置为 **yes**；第二个策略的 **more** 设置为 **no**，表示该策略组结束。数据包的内容必须与这两条策略都匹配，才认为是符合过滤条件 UDP 1701 的。

需要注意的是，当出现 Generic 类型和其他类型混合使用的情况时，若某条 Generic Filter 后的一条业务策略是其他类型（IP Filter 或 IPSSG Filter），这时，即便该条 Generic Filter 的 **more** 设置为 **yes**，也会认为该策略组结束。

配置命令如表 2-23 所示。

操作	命令
设置需要连续检查后续 Generic Filter	**set filter** {**in** | **out**}/*filter-name* **generic more yes**
设置不需要连续检查后续 Generic Filter	**set filter** {**in** | **out**}/*filter-name* **generic more no**
备注：缺省情况下，为不需要连续检查后续 Generic Filter。	

表 2-23 设置是否需要连续检查后续的 Generic Filter

2.1.4.4 Generic Filter 配置指南

为方便起见，本节通过以下实例来说明 Generic Filter 中各个参数的关系及设置方法。这里，不妨假设各个过滤参数的值如下所述：

type=generic；forward=no；offset = 2；length = 8；more = no；compare= equals；mask = 0fffffff000000f0；value = 07fe457000000090。

按上述参数值配置完业务策略之后，假设有个包开始的内容如下：2A 31 97 FE 45 70 12 22 33 99 B4 80 75

如图 2-1 所示，当该数据包和上述 Generic Filter 策略相比较时，因为 **offset** 值为 2，**length** 值为 8，所以需要比较从第三个字节 **97** 开始的 8 个字节中的内容，直到第 10 个字节 **99** 结束。首先将这 8 个字节与 **mask** 的值相与（换成 2 进制计算），得到的结果为 **07fe457000000090**，这个结果即为数据包的比较内容，它与 **value** 的值相等。由于 **compares** 值为 **equals**，因此该数据包匹配此策略，又由于无需检查后续策略（**more** 值为 **no**），因此按照该策略的过滤动作，此数据包将被丢弃。

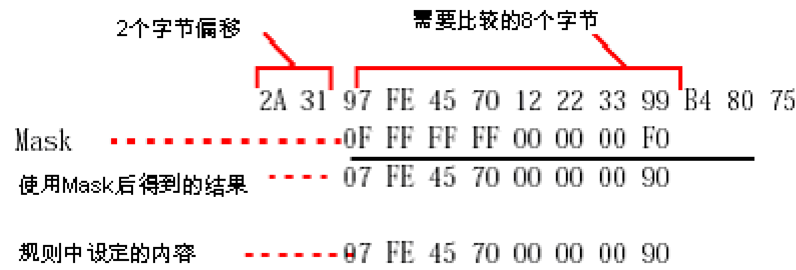


图 2-1 Generic Filter 配置指南

2.2 Filter 全局配置

Filter 全局配置包括以下两个方面内容：

- 启用/禁用业务管理功能
- 设置启用的业务策略组

提示：下述两节配置命令中，“*eth-num*” 代表欲配置的物理端口号，为枚举型数字。取值范围：1，2，3；其中，1 代表 LAN 口，2 代表 WAN 口，3 代表 WAN2/DMZ 口。“*conn-name*”为虚端口对应的连接实例名，由用户在新建连接实例时自定义，具体可参考《HiPER 命令行配置手册 第 4 卷：拨号连接》。在各个配置命令中，不再特别说明这两个参数。

2.2.1 启用/禁用业务管理功能

在配置完所有的业务策略后，必须在需要使用业务管理功能的端口（物理端口或虚端口）上启用 Filter，否则所定义的业务策略根本不会执行。

配置命令如表 2-24 所示。

操作	命令
设置某个物理端口启用业务管理功能	**set interface ethernet/***eth-num* **ip filter enabled**
设置某个物理端口禁用业务管理功能	**set interface ethernet/***eth-num* **ip filter disabled**
设置某个虚端口启用业务管理功能	**set connection/***conn-name* **policy filter enabled**
设置某个虚端口禁用业务管理功能	**set connection/***conn-name* **policy filter disabled**
备注：缺省情况下，为禁用业务管理功能。	

表 2-24 启用/禁用业务管理功能

2.2.2 设置启用的业务策略组

如章节 1.6 中所述，业务策略支持分组功能。用户可以根据实际需要，在不同的端口（物理端口或虚端口）启用不同的业务策略组。对于每一个端口来说，在进入（In）或者外出（Out）方向上可以设置不同的业务策略组，但是，一个方向同时只能设置一个业务策略组。

如果在某个端口启用了某个方向为 In 的业务策略组，那么，该组中的业务策略将作用于从该端口进入 HiPER 的数据包；如果在某个端口启用了某个方向为 Out 的业务策略组，那么，该组中的业务策略将作用于从该端口离开 HiPER 的数据包。

注意，如果某个端口未设置所启用的业务策略组，那么，系统业务策略缺省组中的业务策略（即未定义组名的业务策略）将作用于该端口。

配置命令如表 2-25 所示。

操作	命令
设置某个物理端口启用的方向为 In 的业务策略组	**set interface ethernet/***eth-num* **ip inaclgroup** *filter-groupname*
设置某个物理端口启用的方向为 Out 的业务策略组	**set interface ethernet/***eth-num* **ip outaclgroup** *filter-groupname*
在某个虚端口启用的方向为 In 的业务策略组	**set connection/***conn-name* **policy inaclgroup** *filter-groupname*
在某个虚端口启用的方向为 Out 的业务策略组	**set connection/***conn-name* **policy outaclgroup** *filter-groupname*
备注：*filter-groupname* 的缺省值为空。	

表 2-25 设置启用的业务策略组

2.3 Filter 的显示和诊断

在 HiPER 中，使用命令 **show filter status** *interface* 可以查看指定端口（物理端口或虚端口）启用的所有业务策略（分为进入和外出两个方向）的工作状态，包括各个业务策略的名称、类型、动作、组名、使用次数、匹配次数等信息。

注意，某个端口配置了业务策略后，必须在该端口启用业务管理功能，才会有对应的输出。也就是说，使用命令 **show filter status** *interface* 只能查看到已激活的业务策略的信息。

配置命令如表 2-26 所示。

操作	命令
查看某个物理端口的业务策略工作状态	**show filter status** *interface*
备注：查看物理端口时，*interface* 为物理端口的端口名；取值范围：eth1、eth2、eth3，分别代表 LAN 口、WAN 口、WAN2/DMZ 口。查看虚端口时，*interface* 为虚端口对应的连接实例名，同 *conn-name*。	

表 2-26 查看业务策略工作状态

以下提供了一个使用命令 **show filter status** *interface* 查看业务策略工作状态的实例（如图 2-1），并结合该例对状态信息中各参数进行描述和说明。

```
hiper% show filter status eth1

Incoming filter list status:
Seq   Name    Policy     Type     Group   LstUse  LstMatch      Use     Match

1      lan    Permit    IPSSG    IPSSG       0         0    326992    102650
2      dns    Permit    IPSSG    IPSSG       0         6    224342      8748
3     dhcp    Permit    IPSSG    IPSSG       0      1353    215594       112
4     sina    Permit    IPSSG    IPSSG       0       568    215482        32
5      exe      Deny    IPSSG    IPSSG       0     49793    215450         0
6     pass    Permit    IPSSG    IPSSG       0         0    215450    190965
7 generic     Permit  GENERIC    IPSSG      16        16     24485     24485

no Outgoing filter active.
```

图 2-2 show filter status ***interface*** **使用实例**

如图 2-1 中，显示的信息“ no Outgoing filter active ”表示当前端口在外出方向上未启用任何业务策略；进入方向上启用了若干业务策略，各参数涵义如表 2-27 所示。

参数	涵义
Seq	该业务策略的序号，也代表业务策略的实际执行顺序。
Name	该业务策略的名称。
Policy	该业务策略的动作，Permit-允许；Deny-禁止。
Type	该业务策略的类型，有 IP Filter、IPSSG Filter、GENERIC Filter 三种类型。
Group	该业务策略的组名。
LstUse	该业务策略最近一次被查询距离执行本命令的时间间隔。单位：秒。
LstMatch	该业务策略最近一次被匹配距离执行本命令的时间间隔。单位：秒。
Use	该业务策略被查询的总次数。
Match	该业务策略被匹配的总次数。

表 2-27 show filter status ***interface*** **显示信息描述**

第3章 业务策略配置步骤

3.1 配置步骤

1. 配置各条局部策略

1）新建一条业务策略，确定 Filter 方向，自定义策略名；
2）设置业务策略的类型、动作、组名等；
3）设置业务策略的其余参数。

2. 配置全局策略

出于安全考虑，HiPER 的业务策略体系中默认全局策略的动作是禁止，即与所有业务策略均不匹配的数据包将被丢弃。因此，在配置完所有的局部策略后，一般需要在策略表的最后配置一条全局策略，用来允许其余所有无匹配策略的数据包通过，以保证局域网用户正常上网。

以下提供一个配置全局策略的实例：

！配置全局策略，允许所有没有匹配策略的数据包通过，假设该策略名为 all，方向为进入。

```
new filter in/all
set filter in/all type generic
set filter in/all forward yes
```

3. 在指定端口启用业务管理功能

在配置完所有的业务策略后，必须在需要使用业务管理功能的端口（物理端口或虚端口）上启用 Filter，否则所定义的业务策略根本不会执行。

以下提供一个在 LAN 口启用业务管理功能的实例：

！在 LAN 口启用 Filter

```
set interface ethernet/1 ip filter enabled
```

4. 保存配置

所有的配置完成之后，还需执行命令 **write**，用以保存上述配置。只有执行 **write** 命令之后，当前配置才能保存到 NVRAM 中。如果不执行 **write** 命令，这次改动的配置会在系统重新启动或断电后丢失。

关于配置文件管理的详细描述，请参考手册《HiPER 命令行配置手册 第 1 卷：入门》的章节 3.2。

3.2 插入一条业务策略

如章节 1.5 中所述，所有的业务策略是按照配置的先后顺序存放在业务策略表中的，而 HiPER 在启用业务管理功能之后，当指定端口有数据包通过时，将按照策略表的顺序依次

检查业务策略，看是否由匹配策略。

如果已经配置了若干条业务策略，现需要在其中某条业务策略的前面增加一条业务策略，则需要按以下步骤进行：

1. 在指定端口禁用业务管理功能；
2. 删除全局策略；
3. 删除从新增策略插入位置开始的那一条至最后一条之间对应的所有局部策略；
4. 增加新策略；
5. 按照原先的配置顺序依次增加那几条被删除的局部策略；
6. 增加被删除的全局策略；
7. 在指定端口启用业务管理功能；
8. 保存上述配置。

实例，假设某用户已经按顺序配置了 4 条局部策略（策略名为 1、2、3、4）以及全局策略（策略名为 all），业务策略的方向为 In、作用在 LAN 口。如下所示，具体配置略。

```
new filter in/1
……
new filter in/2
……
new filter in/3
……
new filter in/4
……
new filter in/all
……
set interface ethernet/1 ip filter enabled
```

现在希望在第 3 条策略前加入一条策略（策略名为 5），步骤如下：

1. 在指定端口禁用业务管理功能
   ```
   set interface ethernet/1 ip filter disabled
   ```
2. 删除全局策略 Generic
   ```
   delete filter in/Generic
   ```
3. 删除局部策略 4 和 3
   ```
   delete filter in/4
   delete filter in/3
   ```
4. 增加局部策略 5
   ```
   new filter in/5
   ……
   ```
5. 增加被删除的局部策略 3 和 4
   ```
   new filter in/3
   ……
   new filter in/4
   ……
   ```
6. 增加被删除的全局策略 all

```
new filter in/all
……
```

7. 在指定端口启用业务管理功能
```
set interface ethernet/1 ip filter enabled
```

8. 保存上述配置
```
write
```

3.3 删除一条业务策略

如果已经配置了多条策略，现需要删除其中的某条策略，则需要按以下步骤进行：

1. 在指定端口禁用业务管理功能；
2. 删除全局策略；
3. 删除欲删除的策略至最后一条之间对应的所有局部策略；
4. 按照原先的配置顺序依次增加那几条删除的局部策略，当然，欲删除的策略除外；
5. 增加被删除的全局策略；
6. 在指定端口启用业务管理功能；
7. 保存上述配置。

如果不是按照上述步骤删除策略，而是直接删除其中的某条策略（不是最后一条），那么，该策略所占据的位置将保留，这时如果直接添加一条业务策略，系统会将该策略直接设置到删除策略所在的位置。因此，为避免业务策略的实际顺序与预期顺序不相符合，一般建议按上述步骤删除策略。

实例，假设某用户已经按顺序配置了四条局部策略（策略名为 1、2、3、4）以及全局策略（策略名为 all），业务策略的方向为 In、作用在 LAN 口。如下所示，具体配置略。

```
new filter in/1
……
new filter in/2
……
new filter in/3
……
new filter in/4
……
new filter in/all
……
set interface ethernet/1 ip filter enabled
```

现在希望删除策略 2，步骤如下：

1. 在指定端口禁用业务管理功能
```
set interface ethernet/1 ip filter disabled
```

2. 删除全局策略 all
```
delete filter in/all
```

3. 删除局部策略 4、3 和 2

```
delete filter in/4
delete filter in/3
delete filter in/2
```

4. 增加被删除的局部策略 3 和 4

```
new filter in/3
……
new filter in/4
……
```

5. 增加被删除的全局策略 all

```
new filter in/all
……
```

6. 在指定端口启用业务管理功能

```
set interface ethernet/1 ip filter enabled
```

7. 保存上述配置

```
write
```

第4章　业务策略配置实例

⊕提示：

1. 本章 4.1、4.2 各节提供的实例中，均是将通过 HiPER 的局域网端口（LAN 口）连接到用户局域网，在 LAN 口启用业务管理功能。此外，在章节 4.3 提供了一个在虚端口启用业务管理功能的实例。

2. 本章 4.1、4.2、4.3 各节中都是提供 IPSSG Filter 或者 IP Filter 的配置实例，仅在 4.4 节提供了一个 Generic Filter 的配置实例。

4.1　单个功能配置实例

在本章节中，主要针对 IPSSG Filter 和 IP Filter 两种类型的业务策略，提供一些单个功能配置实例，分别说明各个配置参数的使用方法。

4.1.1 单个功能配置实例——IPSSG Filter

注意，以下各节提供的实例中，ReOS 4.4 以上版本中，过滤源 MAC 地址（章节 4.1.1.5）和设置 IP/MAC 绑定（4.1.1.6）可通过用户管理（IP/MAC 绑定）功能实现，且用户管理功能执行效率更高。

4.1.1.1　过滤源 IP 地址（连续多个）

1　需求

创建 IPSSG Filter 策略，要求允许局域网中 IP 地址在 192.168.1.1～192.168.1.31 范围之内的主机上网。

2　分析

如章节 2.1.2.1 中所述，IPSSG Filter 提供两种方式过滤源地址，方式 1 是通过设置参数 **srcfrom**（源起始 IP 地址）和 **srcend**（源结束 IP 地址）来实现；方式 2 是通过设置参数 **srcaddr**（源 IP 地址）和 **srcmask**（源 IP 掩码）来实现。

方式 1 很简单，无需特别说明。

方式 2 中，通过起始 IP 地址 192.168.1.1 和结束 IP 地址 192.168.1.31 可以计算出这个要过滤的源地址的子网掩码为 255.255.255.224。

3　方式 1 配置步骤

```
new filter in/permit1
set filter in/permit1 type ipssg
set filter in/permit1 forward yes
set filter in/permit1 ipssg srcfrom 192.168.1.1
set filter in/permit1 ipssg srcend 192.168.1.31
```

4 方式 2 配置步骤

```
new filter in/permit2
set filter in/permit2 type ipssg
set filter in/permit2 forward yes
set filter in/permit2 ipssg srcaddr 192.168.1.1
set filter in/permit2 ipssg srcmask 255.255.255.224
```

4.1.1.2 过滤目的 IP 地址（单个）

1 需求

创建 IPSSG Filter 策略，要求禁止局域网中用户访问网站 209.247.228.201。

2 分析

如章节 2.1.2.1 中所述，IPSSG Filter 提供两种方式过滤目的地址，方式 1 是通过设置参数 **destfrom**（目的起始 IP 地址）和 **destend**（目的结束 IP 地址）来实现；方式 2 是通过设置参数 **destaddr**（目的 IP 地址）和 **destmask**（目的 IP 掩码）来实现。

由于欲过滤的目的 IP 地址为单个 IP 地址，因此，方式 1 中需将 **destfrom** 和 **destend** 均设置为同一个 IP 地址；方式 2 中需将 **destmask** 设为 **255.255.255.255**。

3 方式 1 配置步骤

```
new filter in/a
set filter in/a type ipssg
set filter in/a forward no
set filter in/a ipssg destfrom 209.247.228.201
set filter in/a ipssg destend 209.247.228.201
```

4 方式 2 配置步骤

```
new filter in/b
set filter in/b type ipssg
set filter in/b forward no
set filter in/b ipssg destmask 255.255.255.255
set filter in/b ipssg destaddr 209.247.228.201
```

4.1.1.3 过滤目的端口（单个）

1 需求

创建 IPSSG Filter 策略，要求禁止局域网中用户访问 TCP 1863 端口。

2 分析

如章节 2.1.2.3 中所述，IPSSG Filter 提供两种方式过滤目的端口，通过设置参数 **dportfrom**（目的起始端口）和 **dportend**（目的结束端口）来实现；方式 2 是通过设置参数 **destport**（目的端口）和 **destportcmp**（目的端口匹配动作）来实现。

由于欲过滤的目的端口为单个端口，因此，方式 1 中需将 **dportfrom** 和 **dportend** 均设置为同一个端口；方式 2 中需将 **destportcmp** 设为 **eql**。两种方式下，都需要将 **protocol**（协

议类型）设置为 **tcp**（或者 **6**）。

3 方式 1 配置步骤

```
new filter in/1
set filter in/1 type ipssg
set filter in/1 forward no
set filter in/1 ipssg protocol tcp
set filter in/1 ipssg dportfrom 1863
set filter in/1 ipssg dportend 1863
```

4 方式 2 配置步骤

```
new filter in/2
set filter in/2 type ipssg
set filter in/2 forward no
set filter in/2 ipssg protocol tcp
set filter in/2 ipssg destportcmp eql
set filter in/2 ipssg destport 1863
```

4.1.1.4 过滤目的端口（连续多个）

1 需求

创建 IPSSG Filter 策略，要求禁止局域网中用户访问 TCP 4600～4800 端口。

2 分析

如章节 2.1.2.3 中所述，IPSSG Filter 提供两种方式过滤目的端口，通过设置参数 **dportfrom**（目的起始端口）和 **dportend**（目的结束端口）来实现；方式 2 是通过设置参数 **destport**（目的端口）和 **destportcmp**（目的端口匹配动作）来实现。

方式 1 很简单，无需特别说明。

方式 2 中，首先创建一条策略，用于允许访问端口号小于 4600 的所有端口；然后再创建一条策略，用于禁止访问端口号小于 4800 的所有端口。这样，端口号位于 4600～4800 之间的所有端口将被禁止，而端口号大于 4800 的所有端口将被允许。

两种方式下，都需要将 **protocol**（协议类型）设置为 **tcp**（或者 **6**）。

3 方式 1 配置步骤

```
new filter in/denyport1
set filter in/denyport1 type ipssg
set filter in/denyport1 forward no
set filter in/denyport1 ipssg protocol tcp
set filter in/denyport1 ipssg dportfrom 4600
set filter in/denyport1 ipssg dportend 4800
```

4 方始 2 配置步骤

！新建一条业务策略，允许访问小于 4600 的目的端口（使用 TCP 协议）

```
new filter in/denyport21
set filter in/denyport21 type ipssg
```

```
set filter in/denyport21 forward yes
set filter in/denyport21 ipssg protocol 6
set filter in/denyport21 ipssg destportcmp less
set filter in/denyport21 ipssg destport 4600
```

！新建一条业务策略，禁止访问小于 4800 的目的端口（使用 TCP 协议）

```
new filter in/denyport22
set filter in/denyport22 type ipssg
set filter in/denyport22 forward no
set filter in/denyport22 ipssg protocol 6
set filter in/denyport22 ipssg destportcmp less
set filter in/denyport22 ipssg destport 4800
```

4.1.1.5 过滤源 MAC 地址

1 需求

创建 IPSSG Filter 策略，要求禁止局域网中 MAC 地址为 00:07:95:a8:1c:3d 的主机上网。

2 分析

如章节 2.1.2.5 中所述，IPSSG Filter 中，可通过设置参数 **smac**（源 MAC 地址）和 **sneq**（源 MAC 地址比较符）过滤源 MAC 地址。

3 配置步骤

```
new filter in/denymac1
set filter in/denymac1 type ipssg
set filter in/denymac1 forward no
set filter in/denymac1 ipssg smac 000795a81c3d
set filter in/denymac1 ipssg sneq equals
```

4.1.1.6 配置 IP/MAC 绑定

1 需求

创建 IPSSG Filter 策略,实现 IP/MAC 绑定,例如 禁止局域网中 IP 地址为 192.168.1.150、MAC 地址不为 004c5aeefcff 的主机上网。

2 分析

如章节 2.1.2.5 中所述，IPSSG Filter 中，可通过设置参数 **smac**（源 MAC 地址）和 **sneq**（源 MAC 地址比较符）过滤源 MAC 地址。

3 配置步骤

```
new filter in/binding1
set filter in/binding1 type ipssg
set filter in/binding1 forward no
set filter in/binding1 ipssg srcmask 255.255.255.255
set filter in/binding1 ipssg srcaddr 192.168.1.150
```

```
set filter in/binding1 ipssg smac 004c5aeefcff
set filter in/binding1 ipssg sneq notequals
```

4.1.1.7 配置 URL 过滤

1 需求

创建 IPSSG Filter 策略，要求禁止局域网中用户访问整个 sina 站点。

2 分析

如章节 2.1.2.8 中所述，通过参数 **L7filter**（过滤类型）和 **L7key**（过滤内容）设置 URL 过滤，同时，必须将协议设置为 TCP、目的端口设置为 80。

3 配置步骤

```
new filter in/url
set filter in/url type ipssg
set filter in/url forward no
set filter in/url ipssg protocol tcp
set filter in/url ipssg dportfrom 80
set filter in/url ipssg dportend 80
set filter in/url ipssg l7filter url_alg
set filter in/url ipssg l7key sina.com
```

4.1.2 单个功能配置实例——IP Filter

4.1.2.1 过滤源 IP 地址（连续多个）

1 需求

创建一个 IP Filter 策略，要求允许局域网中 IP 地址在 192.168.16.1～192.168.16.31 范围之内的主机上网。

2 分析

如章节 2.1.3.1 中所述，IP Filter 只支持通过设置参数 **srcaddr**（源 IP 地址）和 **srcmask**（源 IP 掩码）来过滤源地址。

通过起始 IP 地址 192.168.1.1 和结束 IP 地址 192.168.16.31 可以计算出这个要过滤的源地址的子网掩码为 255.255.255.224。

3 配置步骤

```
new filter in/test1
set filter in/test1 type ip
set filter in/test1 forward yes
set filter in/test1 ip srcaddr 192.168.16.1
set filter in/test1 ip srcmask 255.255.255.224
```

4.1.2.2 过滤目的 IP 地址（单个）

1 需求

创建 IP Filter 策略，要求禁止局域网中用户访问网站 64.236.24.12。

2 分析

如章节 2.1.3.1 中所述，IP Filter 只支持通过设置参数 **destaddr**（目的 IP 地址）和 **destmask**（目的 IP 掩码）过滤目的 IP 地址。

由于欲过滤的目的 IP 地址为单个 IP 地址，因此需将 **destmask** 设为 **255.255.255.255**。

3 配置步骤

```
new filter in/test2
set filter in/test2 type ip
set filter in/test2 forward no
set filter in/test2 ip destmask 255.255.255.255
set filter in/test2 ip destaddr 64.236.24.12
```

4.1.2.3 过滤目的端口（单个）

1 需求

创建 IP Filter 策略，要求允许局域网中用户访问 UDP 53 端口。

2 分析

如章节 2.1.3.3 中所述，IP Filter 只支持通过设置参数 **destport**（目的端口）和 **destportcmp**（目的端口匹配动作）过滤目的端口。

由于欲过滤的目的端口为单个端口，因此需将 **destportcmp** 设为 **eql**。另外，由于该服务使用 UDP 协议，因此需将 **protocol**（协议类型）设置为 **17**。

3 配置步骤

```
new filter in/test3
set filter in/test3 type ip
set filter in/test3 forward yes
set filter in/test3 ip protocol 17
set filter in/test3 ip destportcmp eql
set filter in/test3 ip destport 53
```

4.1.2.4 过滤目的端口（连续多个）

1 需求

创建 IP Filter 策略，要求禁止局域网中用户访问 TCP 4600～4800 端口。

2 分析

如章节 2.1.3.3 中所述，IP Filter 只支持通过设置参数 **destport**（目的端口）和 **destportcmp**（目的端口匹配动作）过滤目的端口。

实际配置中，首先创建一条策略，用于允许访问端口号小于 4600 的所有端口；然后再创建一条策略，用于禁止访问端口号小于 4800 的所有端口。这样，端口号位于 4600～4800 之间的所有端口将被禁止，而端口号大于 4800 的所有端口将被允许。

3 配置步骤

！新建一条业务策略，允许访问小于 4600 的目的端口（使用 TCP 协议）

```
new filter in/test41
set filter in/test41 type ip
set filter in/test41 forward yes
set filter in/test41 ip protocol 6
set filter in/test41 ip destportcmp less
set filter in/test41 ip destport 4600
```

！新建一条业务策略，禁止访问小于 4800 的目的端口（使用 TCP 协议）

```
new filter in/denyport22
set filter in/denyport22 type ip
set filter in/denyport22 forward no
set filter in/denyport22 ip protocol 6
set filter in/denyport22 ip destportcmp less
set filter in/denyport22 ip destport 4800
```

4.2 典型应用实例

为方便起见，以下各实例中（类型为 IP Filter 或 IPSSG Filter），仅 4.2.1.1 节配置实例中启用了业务管理的分组功能，即为各个业务策略设置了 **groupname**（组名），并在指定端口启用了该业务策略组。其余各配置实例中的业务策略都未启用该功能，如果需要启用该功能，配置方法类似。

4.2.1 过滤目的网站

4.2.1.1 禁止局域网用户访问外网某些网站，允许其他业务

1 需求

某国家有关部门要求如下：禁止国内用户去访问那些违反我国有关规定或者“有问题”的国外站点，例如 http://www.playboy.com、http://www.cnn.com 等等，允许访问其他网站。其中，www.playboy.com、www.cnn.com 对应的 IP 地址分别为 209.247.228.201、64.236.24.12。

2 分析

HiPER 中，提供两种方法过滤目的网站，方法 1 是通过 URL 过滤实现，仅 IPSSG Filter 支持；方法 2 是通过过滤目的 IP 地址实现，IPSSG Filter 和 IP Filter 都支持，这里以 IP Filter 为例进行说明。这里，不妨假设方法 1 中，所设置的系列业务策略的组名均为 group1；方法 2 中，所设置的业务策略的组名均为 group2。

注意，方法 1 中，由于是 URL 过滤，因此需将相关业务策略的协议指定为 TCP、目的

端口指定为 80（详见章节 2.1.2.8）。

3 方法 1 配置步骤

！新建业务策略 example11，用于禁止局域网用户访问 www.playboy.com

```
new filter in/example11
set filter in/example11 type ipssg
set filter in/example11 forward no
set filter in/example11 groupname group1
set filter in/example11 ipssg protocol tcp
set filter in/example11 ipssg dportfrom 80
set filter in/example11 ipssg dportend 80
set filter in/example11 ipssg l7filter url_alg
set filter in/example11 ipssg l7key www.playboy.com
```

！新建业务策略 example12，用于禁止局域网用户访问 www.cnn.com

```
new filter in/example12
set filter in/example12 type ipssg
set filter in/example12 forward no
set filter in/example12 groupname group1
set filter in/example12 ipssg protocol tcp
set filter in/example12 ipssg dportfrom 80
set filter in/example12 ipssg dportend 80
set filter in/example12 ipssg l7filter url_alg
set filter in/example12 ipssg l7key www.cnn.com
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/example13
set filter in/example13 type generic
set filter in/example13 forward yes
set filter in/example13 groupname group1
```

！在 LAN 口启用 Filter 功能、业务策略组 group1

```
set interface ethernet/1 ip filter enabled
set interface ethernet/1 ip inaclgroup group1
```

！保存上述配置

```
write
```

4 方法 2 配置步骤

！新建业务策略 example21，用于禁止局域网用户访问 www.playboy.com

```
new filter in/example21
set filter in/example21 type ip
set filter in/example21 forward no
set filter in/example21 groupname group2
set filter in/example21 ip destmask 255.255.255.255
set filter in/example21 ip destaddr 209.247.228.201
```

！新建业务策略 example12，用于禁止局域网用户访问 www.cnn.com

```
new filter in/example22
set filter in/example22 type ip
set filter in/example22 forward no
set filter in/example22 groupname group2
set filter in/example22 ip destmask 255.255.255.255
set filter in/example22 ip destaddr 64.236.24.12
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/example23
set filter in/example23 type generic
set filter in/example23 forward yes
set filter in/example23 groupname group2
```

！在 LAN 口启用 Filter 功能、业务策略组 group2

```
set interface ethernet/1 ip filter enabled
set interface ethernet/1 ip inaclgroup group2
```

！保存上述配置

```
write
```

4.2.1.2 允许局域网用户访问某些网站，禁止访问其他网站

1 需求

某公司要求如下：只允许局域网用户访问以下地址段的网站，202.0.0.0/8、218.0.0.0/8 以及 211.0.0.0/8，禁止访问其他地址段的网站。

2 分析

IPSSG Filter 和 IP Filter 都支持过滤目的 IP 地址，这里以 IPSSG Filter 为例说明。实例中，允许访问的三个地址段均为 C 类子网，因此 **destmask**（目的 IP 掩码）的值都为 **255.0.0.0**。

3 配置步骤

！新建 filter 策略 1，用于允许访问 202.0.0.0/8 网段

```
new filter in/1
set filter in/1 type ipssg
set filter in/1 forward yes
set filter in/1 ipssg destmask 255.0.0.0
set filter in/1 ipssg destaddr 202.0.0.0
```

！新建业务策略 2，用于允许访问 218.0.0.0/8

```
new filter in/2
set filter in/2 type ipssg
set filter in/2 forward yes
set filter in/2 ipssg destmask 255.0.0.0
set filter in/2 ipssg destaddr 218.0.0.0
```

！新建 filter 策略 3，用于允许访问 211.0.0.0/8

```
new filter in/3
set filter in/3 type ipssg
```

```
set filter in/3 forward yes
set filter in/3 ipssg destmask 255.0.0.0
set filter in/3 ipssg destaddr 211.0.0.0
```

！新建 filter 策略 4，用于禁止访问其他网站

```
new filter in/4
set filter in/4 type ipssg
set filter in/4 forward no
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/5
set filter in/5 type generic
set filter in/5 forward yes
```

！在 LAN 口启用业务管理功能

```
set interface ethernet/1 ip filter enabled
```

！保存上述配置

```
write
```

4.2.2 过滤源 IP 地址

4.2.2.1 允许局域网某些用户访问 Internet，禁止其他用户访问 Internet

1 需求

某局域网用户使用的 IP 地址段为 192.168.1.0/24，现要求如下：允许使用 IP 地址为 192.168.1.1/24 ~192.168.1.31/24 的用户上网，禁止其他 IP 地址的用户上网。

2 分析

IPSSG Filter 和 IP Filter 都支持过滤源 IP 地址。

IPSSG Filter 支持两种方式过滤源地址，方式 1 是通过设置参数 **srcfrom**（源起始 IP 地址）和 **srcend**（源结束 IP 地址）来实现；方式 2 是通过设置参数 **srcaddr**（源 IP 地址）和 **srcmask**（源 IP 掩码）来实现。IP Filter 仅支持第 2 种方式，即通过设置参数 **srcaddr**（源 IP 地址）和 **srcmask**（源 IP 掩码）来过滤源 IP 地址。

以下将提供上述两种方式的配置步骤，方式 1 以 IPSSG Filter 为例进行说明，方式 2 以 IP Filter 为例进行说明。

3 方式 1 配置步骤

！新建业务策略 1，用于允许 IP 地址为 192.168.1.1/24~192.168.1.31/24 内的用户上网

```
new filter in/1
set filter in/1 type ipssg
set filter in/1 forward yes
set filter in/1 ipssg srcfrom 192.168.1.1
set filter in/1 ipssg srcend 192.168.1.31
```

！新建 filter 策略 2，禁止其他用户上网

```
new filter in/2
```

```
set filter in/2 type ipssg
set filter in/2 forward no
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/3
set filter in/3 type generic
set filter in/3 forward yes
```

！在 LAN 口启用业务管理功能

```
set interface ethernet/1 ip filter enabled
```

！保存上述配置

```
write
```

4 方式 2 配置步骤

！新建业务策略 1，用于允许 IP 地址为 192.168.1.1/24~192.168.1.31/24 内的用户上网

```
new filter in/1
set filter in/1 type ip
set filter in/1 forward yes
set filter in/1 ip srcmask 255.255.255.224
set filter in/1 ip srcaddr 192.168.1.1
```

！新建业务策略 2，禁止其他用户上网

```
new filter in/2
set filter in/2 type ip
set filter in/2 forward no
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/3
set filter in/3 type generic
set filter in/3 forward yes
```

！在 LAN 口启用业务管理功能

```
set interface ethernet/1 ip filter enabled
```

！保存上述配置

```
write
```

4.2.3 过滤局域网用户的服务

4.2.3.1 禁止在内网使用 MSN 聊天

1. 需求

某公司希望禁止公司局域网用户使用 MSN 聊天。本实例以 MSN 7.0 为例说明，MSN 7.0 版本使用 TCP 1863 端口、以及 IP 地址为 65.54.0.1~65.54.255.254 范围内的 TCP 443 端口。

分析

如章节 2.1.2.3 和章节 2.1.3.3 中所述，IPSSG Filter 和 IP Filter 都支持过滤目的端口，这里以 IPSSG Filter 为例进行说明。

2. 配置步骤

！新建业务策略 1，禁止局域网用户访问 TCP 1863 端口

```
new filter in/1
set filter in/1 type ipssg
set filter in/1 forward no
set filter in/1 ipssg protocol tcp
set filter in/1 ipssg dportfrom 1863
set filter in/1 ipssg dportend 1863
```

！新建业务策略 2，禁止局域网用户访问 65.54.0.1~65.54.255.254 的 TCP 443 端口

```
new filter in/2
set filter in/2 type ipssg
set filter in/2 forward no
set filter in/2 ipssg protocol tcp
set filter in/2 ipssg destfrom 65.54.0.1
set filter in/2 ipssg destend 65.54.255.254
set filter in/2 ipssg dportfrom 443
set filter in/2 ipssg dportend 443
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/3
set filter in/3 type generic
set filter in/3 forward yes
```

！在 LAN 口启用业务管理功能

```
set interface ethernet/1 ip filter enabled
```

！保存上述配置

```
write
```

4.2.3.2 防冲击波/震荡波病毒

1. 需求

冲击波/震荡波病毒是当前互联网中比较泛滥而且极度消耗网络资源的病毒，建议在 HiPER 中加以屏蔽。可通过关闭 TCP 135、137、139、445、1025、5554、9996 端口来实现。

2. 分析

如章节 2.1.2.3 和章节 2.1.3.3 中所述，IPSSG Filter 和 IP Filter 都支持过滤目的端口，这里以 IP Filter 为例进行说明。

3. 配置步骤

！新建业务策略 1，禁止局域网用户访问 TCP 135 端口

```
new filter in/1
set filter in/1 type ip
set filter in/1 forward no
set filter in/1 ip protocol 6
set filter in/1 ip destport 135
```

```
set filter in/1 ip destportcmp eql
```

！新建业务策略 2，禁止局域网用户访问 TCP 137 端口

```
new filter in/2
set filter in/2 type ip
set filter in/2 forward no
set filter in/2 ip protocol 6
set filter in/2 ip destport 137
set filter in/2 ip destportcmp eql
```

！新建业务策略 3，禁止局域网用户访问 TCP 139 端口

```
new filter in/3
set filter in/3 type ip
set filter in/3 forward no
set filter in/3 ip protocol 6
set filter in/3 ip destport 139
set filter in/3 ip destportcmp eql
```

！新建业务策略 4，禁止局域网用户访问 TCP 445 端口

```
new filter in/4
set filter in/4 type ip
set filter in/4 forward no
set filter in/4 ip protocol 6
set filter in/4 ip destport 445
set filter in/4 ip destportcmp eql
```

！新建业务策略 5，禁止局域网用户访问 TCP 1025 端口

```
new filter in/5
set filter in/5 type ip
set filter in/5 forward no
set filter in/5 ip protocol 6
set filter in/5 ip destport 1025
set filter in/5 ip destportcmp eql
```

！新建业务策略 6，禁止局域网用户访问 TCP 5554 端口

```
new filter in/6
set filter in/6 type ip
set filter in/6 forward no
set filter in/6 ip protocol 6
set filter in/6 ip destport 5554
set filter in/6 ip destportcmp eql
```

！新建业务策略 7，禁止局域网用户访问 TCP 9996 端口

```
new filter in/7
set filter in/7 type ip
set filter in/7 forward no
set filter in/7 ip protocol 6
set filter in/7 ip destport 9996
set filter in/7 ip destportcmp eql
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/8
set filter in/8 type generic
set filter in/8 forward yes
```

！在 LAN 口启用业务管理功能

```
set interface ethernet/1 ip filter enabled
```

！保存上述配置

```
write
```

4.2.4 配置基于时间的 Filter 策略

4.2.4.1 禁止内网某些用户在特定时间对 Internet 的访问

1. 需求

某公司对 IP 地址为 192.168.1.114 的用户制订的上网要求如下：

在工作时间内，禁止该用户使用 FTP 传输文件（TCP 21 端口），允许其他上网业务。在休息时间内，禁止该用户对 Internet 的所有访问。

假设上述规定在 2005 年度有效，工作时间为：星期一～星期五，上午 09:00:00～11:59:59，下午 1:00:00～5:59:59；其余时间为休息时间。

2. 分析

这里对时间段的配置进行简单分析，时间段配置的详细说明请参考手册《HiPER 命令行配置手册 第 2 卷：基本配置》的第 4 章（时间段配置）。

根据该公司的规定，时间段生效的起始时间为 2005 年 1 月 1 日凌晨零点零分，结束时间为 2005 年 12 月 31 日 23:59:59。

工作时间可以分为两个时间单元：

1. 星期一～星期五，09:00:00～11:59:59；
2. 星期一～星期五，13:00:00～17:59:59。

休息时间可以分为四个时间单元：

1. 星期一～星期五，00:00:00～08:59:59；
2. 星期一～星期五，12:00:00～12:59:59；
3. 星期一～星期五，18:00:00～23:59:59；
4. 星期六～星期天，00:00:00～23:59:59。

3. 配置步骤

！配置时间段策略 worktime——工作时间

```
new timerange/worktime
set timerange/worktime tmstart 2005-1-1  0:00:00
set timerange/worktime tmstop 2005-12-31 23:59:59
set timerange/worktime 1stperiod type weekday
set timerange/worktime 1stperiod begin 09:00:00
set timerange/worktime 1stperiod end 11:59:59
set timerange/worktime 2ndperiod type weekday
```

```
set timerange/worktime 2ndperiod begin 13:00:00
set timerange/worktime 2ndperiod end 17:59:59
```

！配置时间段策略 freetime——休息时间

```
new timerange/freetime
set timerange/freetime tmstart 2005-1-1  0:00:00
set timerange/freetime tmstop 2005-12-31 23:59:59
set timerange/freetime 1stperiod type weekday
set timerange/freetime 1stperiod begin 00:00:00
set timerange/freetime 1stperiod end 08:59:59
set timerange/freetime 2ndperiod type weekday
set timerange/freetime 2ndperiod begin 12:00:00
set timerange/freetime 2ndperiod end 12:59:59
set timerange/freetime 3rdperiod type weekday
set timerange/freetime 3rdperiod begin 18:00:00
set timerange/freetime 3rdperiod end 23:59:59
set timerange/freetime 4thperiod type weekend
set timerange/freetime 4thperiod begin 00:00:00
set timerange/freetime 4thperiod end 23:59:59
```

！配置业务策略 1，禁止该用户（192.168.1.114）在工作时间内访问 TCP 21 端口

```
new filter in/1
set filter in/1 type ipssg
set filter in/1 forward no
set filter in/1 ipssg timerange worktime
set filter in/1 ipssg srcmask 255.255.255.255
set filter in/1 ipssg srcaddr 192.168.1.114
set filter in/1 ipssg protocol 6
set filter in/1 ipssg destport 21
set filter in/1 ipssg destportcmp eql
```

！配置业务策略 2，允许该用户（192.168.1.114）在工作时间内使用其他所有上网业务

```
new filter in/2
set filter in/2 type ipssg
set filter in/2 forward yes
set filter in/2 ipssg timerange worktime
set filter in/2 ipssg srcmask 255.255.255.255
set filter in/2 ipssg srcaddr 192.168.1.114
```

！配置业务策略 3，禁止该用户（192.168.1.114）在休息时间使用任何上网业务

```
new filter in/3
set filter in/3 type ipssg
set filter in/3 forward no
set filter in/3 ipssg timerange freetime
set filter in/3 ipssg srcmask 255.255.255.255
set filter in/3 ipssg srcaddr 192.168.1.114
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/4
set filter in/4 type generic
set filter in/4 forward yes
```

！在 LAN 口启用 Filter

```
set interface ethernet/1 ip filter enabled
```

！保存

```
write
```

4.2.5 过滤源端口

4.2.5.1 允许某些外网用户访问局域网服务器，禁止其他外网用户访问

1. 需求

某局域网一台 Microsoft SQL Server（IP 地址为 192.168.1.100），microsoft sql server 使用 TCP 1433 端口。假设 Hiper 的 LAN 口的 IP 地址为 192.168.1.1，WAN 口的 IP 地址为 211.21.21.21，并且，在 WAN 口启用 NAT 功能。

要求：允许 Internet 上 IP 地址为 218.1.21.1~218.1.21.6 范围内的主机可访问该服务器，禁止 Internet 上的其他所有用户访问该服务器。

2. 分析

本实例中，首先需要通过配置 NAT 静态映射实现通过 Internet 访问该 SQL Server，然后再通过配置业务策略来实现允许 218.1.21.1~218.1.21.6 的主机访问该 SQL Server，并禁止其他所有用户访问该 SQL Server。

关于 NAT 静态映射的配置说明请参考手册《HiPER 命令行配置手册 第 5 卷 NAT 配置》的章节 3.3（NAT 静态映射配置）。

3. NAT 静态映射配置步骤

！新建一条 NAT 静态映射 sql，实现通过 Internet 访问该 SQL Server，这里假设该 NAT 静态映射绑定的 NAT 规则名为 ETHbind

```
new ip nat static/sql
set ip nat static/sql enabled yes
set ip nat static/sql protocol tcp
set ip nat static/sql dstport 1433
set ip nat static/sql localport 1433
set ip nat static/sql localaddress 192.168.1.100
set ip nat static/sql binding ETHbind
```

4. 业务策略配置步骤

！新建业务策略 1，允许 Internet 上 218.1.21.1~218.1.21.6 内的主机访问该服务器

```
new filter in/1
set filter in/1 enabled yes
set filter in/1 type ipssg
set filter in/1 ipssg srcfrom 192.168.1.100
```

```
set filter in/1 ipssg srcend 192.168.1.100
set filter in/1 ipssg destfrom 218.1.21.1
set filter in/1 ipssg destend 218.1.21.6
set filter in/1 ipssg protocol tcp
set filter in/1 ipssg sportfrom 1433
set filter in/1 ipssg sportend 1433
```

！新建业务策略 2，禁止其他所有外网用户访问该服务器

```
new filter in/2
set filter in/2 enabled yes
set filter in/2 type ipssg
set filter in/2 forward no
set filter in/2 ipssg srcfrom 192.168.1.100
set filter in/2 ipssg srcend 192.168.1.100
set filter in/2 ipssg protocol tcp
set filter in/2 ipssg sportfrom 1433
set filter in/2 ipssg sportend 1433
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/3
set filter in/3 type generic
set filter in/3 forward yes
```

！在 LAN 口启用 Filter

```
set interface ethernet/1 ip filter enabled
```

！保存配置

```
write
```

4.2.6 配置 TCP 单向访问连接

4.2.6.1 限制 TCP 连接只能由指定网络中的主机发起

1 需求

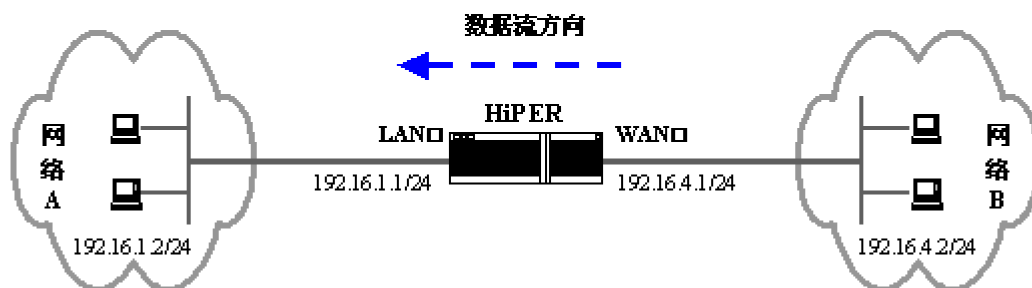


图 4-2 配置 TCP 单向访问连接——方案图

如图 4-2 所示，通过 HiPER 连接两个网络，其中，网络 A 与 LAN 口相连，网络 B 与 WAN 口相连。注意，本实例中，HiPER 未启用 NAT 功能。

要求如下：允许网络 A 的所有主机初始化到网络 B 的 TCP 通信，禁止网络 B 的任何主机初始化到网络 A 的 TCP 通信，不限制其他应用。

2 分析

这里，需要过滤从网络 B 发起经过 HiPER 转发到网络 A 的流量，对于这个方向上的 TCP 连接，需要检查 TCP 报文是否是初始化连接报文，即检查 ACK 或者 RST 标志是否置位。如果 ACK 或者 RST 已经置位，则表示该 TCP 报文不是初始化连接报文，而是已经建立了 TCP 连接的报文，将被允许通过；如果 ACK 或 RST 均未置位，则表示该 TCP 报文为初始化连接报文，将被禁止通过。对于这个方向上的其他应用，则不限制。

可通过 3 条策略实现上述需求：

首先创建业务策略 1，用于允许由网络 A 中的主机主动发起的 TCP 连接的返回报文通过。

然后创建业务策略 2，用于禁止其他 TCP 连接报文通过，即禁止由网络 B 中的主机主动发起的 TCP 连接的报文通过。

之后，需创建一条全局策略 3，用于允许其他所有数据包通过。

由于系统未启用 NAT 功能，因此，可在 HiPER 的 LAN 口或者 WAN 口启用 Filter 功能。若在 LAN 口启用 Filter 功能（方式 1），则 Filter 的方向为 Out；若在 WAN 口启用（方式 2），则 Filter 的方向为 In。以下分别说明这两种情况，其中，方式 1 以 IPSSG Filter 为例说明；方式 2 以 IP Filter 为例说明。

3 方式 1 配置步骤

！新建一条业务策略 1，允许由网络 A 的主机发起的 TCP 连接的返回报文通过

```
new filter out/1
set filter out/1 type ipssg
set filter out/1 forward yes
set filter out/1 ipssg protocol tcp
set filter out/1 ipssg tcpestab Yes
```

！新建一条业务策略 2， 禁止由网络 B 的主机发起的 TCP 连接的报文通过

```
new filter out/2
set filter out/2 type ipssg
set filter out/2 forward no
set filter out/2 ipssg protocol tcp
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter out/3
set filter out/3 type generic
set filter out/3 forward yes
```

！在 LAN 口启用 Filter

```
set interface ethernet/1 ip filter enabled
```

！保存上述配置

```
write
```

4 方式 2 配置步骤

！新建一条业务策略 1，允许由网络 A 的主机发起的 TCP 连接的返回报文通过

```
new filter in/1
set filter in/1 type ip
set filter in/1 forward yes
set filter in/1 ip protocol 6
set filter in/1 ip tcpestab Yes
```

！新建一条业务策略 2，禁止由网络 B 的主机发起的 TCP 连接的报文通过

```
new filter in/2
set filter in/2 type ip
set filter in/2 forward no
set filter in/2 ip protocol 6
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/3
set filter in/3 type generic
set filter in/3 forward yes
```

！在 WAN 口启用 Filter 功能

```
set interface ethernet/2 ip filter enabled
```

！保存上述配置

```
write
```

4.3 虚端口启用业务管理功能应用实例

1 需求

某公司总部在上海，该公司有一些出差和远程办公的移动用户通过 L2TP VPN 隧道在远程访问总公司局域网内部资源。要求如下：防止移动用户中了冲击波病毒之后，病毒通过 L2TP VPN 隧道攻击 HiPER 及总公司局域网内部主机。

注意，这里只提供与业务管理功能相关的配置。本实例中，假定 HiPER 只建立了 3 条 L2TP VPN 隧道，连接实例名分别为 con1、con2、con3。实际应用中，可能会远远大于这个数量，但配置方法却是类似的。

2 分析

如章节 4.2.3.2 实例，可通过关闭 TCP 135、137、139、445、1025、5554、9996 端口来实现防冲击波病毒。这里以 IPSSG Filter 为实例进行说明，并假设业务策略的组名都为 group1。

由于冲击波病毒是感染病毒的移动用户通过 L2TP VPN 隧道进行攻击的，所以只能在各个虚端口（即连接实例）上启用业务管理功能，从而防止攻击。

3 配置步骤

！新建业务策略 cjb1，禁止移动用户访问 TCP 135 端口

```
new filter in/cjb1
set filter in/cjb1 groupname group1
set filter in/cjb1 type ipssg
set filter in/cjb1 forward no
set filter in/cjb1 ipssg protocol tcp
```

```
set filter in/cjb1 ipssg dportfrom 135
set filter in/cjb1 ipssg dportend 135
```

！新建业务策略 cjb2，禁止移动用户访问 TCP 139 端口

```
new filter in/cjb2
set filter in/cjb2 groupname group1
set filter in/cjb2 type ipssg
set filter in/cjb2 forward no
set filter in/cjb2 ipssg protocol tcp
set filter in/cjb2 ipssg dportfrom 139
set filter in/cjb2 ipssg dportend 139
```

！新建业务策略 cjb3，禁止移动用户访问 TCP 445 端口

```
new filter in/cjb3
set filter in/cjb3 groupname group1
set filter in/cjb3 type ipssg
set filter in/cjb3 forward no
set filter in/cjb3 ipssg protocol tcp
set filter in/cjb3 ipssg dportfrom 445
set filter in/cjb3 ipssg dportend 445
```

！新建业务策略 cjb4，禁止移动用户访问 TCP 1025 端口

```
new filter in/cjb4
set filter in/cjb4 groupname group1
set filter in/cjb4 type ipssg
set filter in/cjb4 forward no
set filter in/cjb4 ipssg protocol tcp
set filter in/cjb4 ipssg dportfrom 1025
set filter in/cjb4 ipssg dportend 1025
```

！新建业务策略 cjb5，禁止移动用户访问 TCP 9996 端口

```
new filter in/cjb5
set filter in/cjb5 groupName group1
set filter in/cjb5 type ipssg
set filter in/cjb5 forward no
set filter in/cjb5 ipssg protocol tcp
set filter in/cjb5 ipssg dportfrom 9996
set filter in/cjb5 ipssg dportend 9996
```

！新建业务策略 cjb6，禁止移动用户访问 TCP 137 端口

```
new filter in/cjb6
set filter in/cjb6 groupname group1
set filter in/cjb6 type ipssg
set filter in/cjb6 forward no
set filter in/cjb6 ipssg protocol tcp
set filter in/cjb6 ipssg dportfrom 137
set filter in/cjb6 ipssg dportend 137
```

！新建业务策略 cjb7，禁止移动用户访问 TCP 5554 端口

```
new filter in/cjb7
set filter in/cjb7 groupname group1
set filter in/cjb7 type ipssg
set filter in/cjb7 forward no
set filter in/cjb7 ipssg protocol tcp
set filter in/cjb7 ipssg dportfrom 5554
set filter in/cjb7 ipssg dportend 5554
```

！设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/all
set filter in/all type generic
set filter in/all groupname group1
set filter in/all forward yes
```

！在连接实例 con1 启用 Filter 功能、业务策略组 group1

```
set connection/con1 policy filter enabled
set connection/con1 policy inaclgroup group1
```

！在连接实例 con2 启用 Filter 功能、业务策略组 group1

```
set connection/con2 policy filter enabled
set connection/con2 policy inaclgroup group1
```

！在连接实例 con3 启用 Filter 功能、业务策略组 group1

```
set connection/con3 policy filter enabled
set connection/con3 policy inaclgroup group1
```

！保存上述配置

```
write
```

4.4 Generic Filter 配置实例

1 需求

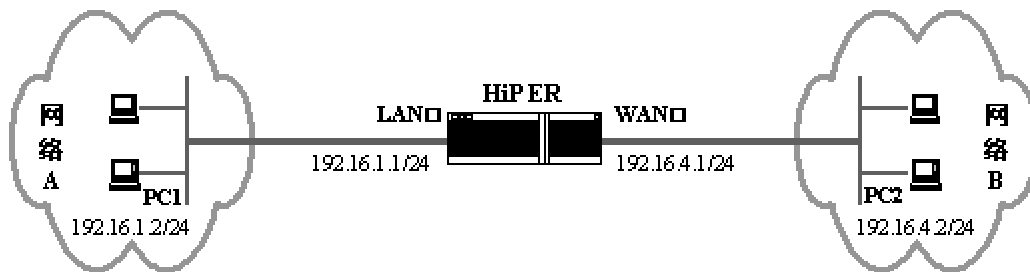


图 4-3 Generic Fitler 配置实例——方案图

如图 4-3 所示，通过 HiPER 连接两个网络，其中，网络 A 与 LAN 口相连，网络 B 与 WAN 口相连。PC1 为网络 A 中的一台主机，PC2 为网络 B 中的一台主机。HiPER 及这两台主机的 IP 地址如下：

HiPER 的 LAN 口：192.16.1.1/24

HiPER 的 WAN 口：192.16.4.1/24

网络 A 中的 PC1：192.16.1.2/24

网络 B 中的 PC2：192.16.4.2/24

要求如下：

a) 只禁止 PC1 Ping PC2（注意，允许 PC2 Ping PC1）；
b) PC1 其他应用不受影响；
c) PC2 其他应用不受影响；
d) 和 PC1 同一网络的其他 PC 访问 PC2 不受影响。

2 分析

上述要求实际上就是只禁止 PC1 Ping PC2，允许网络 A 和网络 B 的主机之间的其他任何访问。

禁止 PC1 Ping PC2，也就是禁止 PC1 向 PC2 发送 ICMP 的 echo ping request（对应的类型字段为 8）数据包，对该数据包的分析如表 4-1。如果某个数据包符合表 4-1 中的过滤条件，则可以唯一确定它就是 PC1 向 PC2 发送 ICMP 的 echo ping request 包。

参数值 / 过滤目标	Offset	Length	Value（16 进制）
协议类型（ICMP）	23	1	01
源 IP 地址（192.16.1.2）	26	4	C0 10 01 02
目的 IP 地址（192.16.4.2）	30	4	C0 10 04 02
ICMP 的 Type 字段（8）	34	1	08

表 4-1 Generic Fitler 配置实例——echo ping request 包分析

从表 4-1 中，可以看出，协议类型、Type 字段分别需要设置一个业务策略过滤；源 IP 地址和目的 IP 地址位置相邻，共 8 个字节，因此只需一个策略就能同时过滤它们。这 3 个连续的策略构成一个业务策略组,并且,需将前 2 条策略设置为需要连续检查后续策略(**more** 设置为 **yes**)，将最后一条策略设置为不需要连续检查后续策略（**more** 设置为 **no**）。

然后，还需设置一条全局策略，其余所有无匹配策略的数据包通过，当然也就允许了网络 A 和网络 B 的主机之间的其他任何访问。

3 配置步骤

！配置业务策略 request，过滤 ICMP 的 Type 字段（值为 8）

```
new filter in/request
set filter in/request forward no
set filter in/request type generic
set filter in/request generic offset 34
set filter in/request generic length 1
set filter in/request generic mask ff
set filter in/request generic value 08
set filter in/request generic compare equals
set filter in/request generic more yes
```

！配置业务策略 icmp，过滤 ICMP 协议

```
new filter in/icmp
set filter in/icmp forward no
```

```
set filter in/icmp type generic
set filter in/icmp generic offset 23
set filter in/icmp generic length 1
set filter in/icmp generic mask ff
set filter in/icmp generic value 01
set filter in/icmp generic compare equals
set filter in/icmp generic more yes
```

！配置业务策略 addr，过滤源 IP 地址 192.16.1.2 和目的 IP 地址 192.16.4.2

```
new filter in/addr
set filter in/addr forward no
set filter in/addr type generic
set filter in/addr generic offset 26
set filter in/addr generic length 8
set filter in/addr generic mask ffffffffffffffff
set filter in/addr generic value c0100102c0100402
set filter in/addr generic compare equals
set filter in/addr generic more no
```

！设置全局策略 all，允许其他所有数据包（必须有，且最后设置）

```
new filter in/all
set filter in/all type generic
set filter in/all forward yes
```

！在 LAN 口启用业务管理功能

```
set interface ethernet/1 ip filter enabled
```

！保存上述配置

```
write
```

附录一 常用 IP 协议号

协议	协议号	全称
IP	0	Internet Protocol
ICMP	1	Internet Protocol Message Protocol
IGMP	2	Internet Group Management
GGP	3	Gateway-Gateway Protocol
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Porotocl
PUP	12	PARC Universal Packet Protocol
UDP	17	User Datagram Protocl
HMP	20	Host Monitoring Protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	Reliable Datagram Protocol
GRE	47	General Routing Encapsulation
ESP	50	Encap Security Payload
AH	51	Authentication Header
RVD	66	MIT Remote Virtual Disk
EIGRP	88	Enhandced Interior Gateway Routing Portocol
OSPF	89	Open Shortest Path First

附录二 常用 TCP/UDP 端口号

服务	端口号	协议	描述
echo	7	tcp	
echo	7	udp	
discard	9	tcp	
discard	9	udp	
systat	11	tcp	Active users
systat	11	udp	Active users
daytime	13	tcp	
daytime	13	udp	
qotd	17	tcp	Quote of the day
qotd	17	udp	Quote of the day
chargen	19	tcp	Character generator
chargen	19	udp	Character generator
ftp-data	20	tcp	FTP, data
ftp	21	tcp	FTP. control
telnet	23	tcp	
smtp	25	tcp	Simple Mail Transfer Protocol
time	37	tcp	timserver
time	37	udp	timserver
rlp	39	udp	Resource Location Protocol
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nicname	43	tcp	whois
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
bootps	67	udp	Bootstrap Protocol Server

bootpc	68	udp	Bootstrap Protocol Client
tftp	69	udp	Trivial File Transfer
gopher	70	tcp	
finger	79	tcp	
http	80	tcp	World Wide Web
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
hostname	101	tcp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
rtelnet	107	tcp	Remote Telnet Service
pop2	109	tcp	Post Office Protocol - Version 2
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Identification Protocol
uucp-path	117	tcp	
nntp	119	tcp	Network News Transfer Protocol
ntp	123	udp	Network Time Protocol
epmap	135	tcp	DCE endpoint resolution
epmap	135	udp	DCE endpoint resolution
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
imap	143	tcp	Internet Message Access Protocol
pcmail-srv	158	tcp	PCMail Server
snmp	161	udp	
snmptrap	162	udp	SNMP trap
print-srv	170	tcp	Network PostScript
bgp	179	tcp	Border Gateway Protocol

irc	194	tcp	Internet Relay Chat Protocol
ipx	213	udp	IPX over IP
ldap	389	tcp	Lightweight Directory Access Protocol
https	443	tcp	MCom
https	443	udp	MCom
microsoft-ds	445	tcp	
microsoft-ds	445	udp	
kpasswd	464	tcp	Kerberos (v5)
kpasswd	464	udp	Kerberos (v5)
isakmp	500	udp	Internet Key Exchange
exec	512	tcp	Remote Process Execution
biff	512	udp	
login	513	tcp	Remote Login
who	513	udp	
cmd	514	tcp	
syslog	514	udp	
printer	515	tcp	
talk	517	udp	
ntalk	518	udp	
efs	520	tcp	Extended File Name Server
router	520	udp	route routed
timed	525	udp	
tempo	526	tcp	
courier	530	tcp	
conference	531	tcp	
netnews	532	tcp	
netwall	533	udp	For emergency broadcasts
uucp	540	tcp	
klogin	543	tcp	Kerberos login
kshell	544	tcp	Kerberos remote shell

new-rwho	550	udp	
remotefs	556	tcp	
rmonitor	560	udp	
monitor	561	udp	
ldaps	636	tcp	LDAP over TLS/SSL
doom	666	tcp	Doom Id Software
doom	666	udp	Doom Id Software
kerberos-adm	749	tcp	Kerberos administration
kerberos-adm	749	udp	Kerberos administration
kerberos-iv	750	udp	Kerberos version IV
kpop	1109	tcp	Kerberos POP
phone	1167	udp	Conference calling
ms-sql-s	1433	tcp	Microsoft-SQL-Server
ms-sql-s	1433	udp	Microsoft-SQL-Server
ms-sql-m	1434	tcp	Microsoft-SQL-Monitor
ms-sql-m	1434	udp	Microsoft-SQL-Monitor
wins	1512	tcp	Microsoft Windows Internet Name Service
wins	1512	udp	Microsoft Windows Internet Name Service
ingreslock	1524	tcp	
l2tp	1701	udp	Layer Two Tunneling Protocol
pptp	1723	tcp	Point-to-point tunnelling protocol
radius	1812	udp	RADIUS authentication protocol
radacct	1813	udp	RADIUS accounting protocol
nfsd	2049	udp	NFS server
knetd	2053	tcp	Kerberos de-multiplexor
man	9535	tcp	Remote Man Server

附录三 图附录

附录四 表目录